OV303R6

User Manual

Contents

1 Safety Precautions 1
2 Overview 2
2.1 Application 2
2.2 Features 2
2.3 Standards Compatibility and Compliance 3
3 Hardware Description and Hardware Installation 4
3.1 Hardware Description 4
3.1.1 Front Panel 4
3.1.2 Rear Panel 5
3.2 Hardware Installation 5
4 PC Network Configuration and Login 7
4.1 PC Network Configuration 7
4.2 Logging in to the DSL Router 9
5 Web-Based Management 10
5.1 Device Information 10
5.1.1 Summary 10
5.2 Quick Setup 11
5.3 Advanced Setup 12
5.3.1 Layer2 Interface 12
5.3.2 WAN Service 15
5.3.3 LAN Configuration 43
5.3.4 NAT 48
5.3.5 Security 54
5.3.6 Parental Control 58
5.3.7 Quality of Service 60
5.3.8 Routing 64
5.3.9 DSL 68
5.3.10 UPnP 68
5.3.11 DNS Proxy 69
5.3.12 IP Tunnel 70
5.4 Diagnostics 71
5.5 Management 72

5.5.1 Settings 72
5.5.2 System Log..... 73
5.5.3 TR-069 Client 75
5.5.4 Access Control 76
5.5.5 Update Software 77
5.5.6 Reboot 78

1 Safety Precautions

Read the following information carefully before operating the device. Follow the
precaution items below to protect the device from risks and damage caused by fire and electric power.

- Use the type of power marked in the volume label.
- Use the power adapter in the device package.
- Pay attention to the power load of outlets or prolonged lines. An overburden power outlet or damaged line and plug may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it at once.
- Space is necessary for heat dissipation to avoid damage caused by overheating of the device. The holes on the device are designed for heat dissipation to ensure that the device works normally. Do not cover these heat dissipation holes.
- Do not put this device close to a heat source or under a high temperature. Keep the device away from direct sunlight.
- Do not put this device close to a damp place. Do not spill any fluid on this device.
- Unless instructed by our customer engineer or your broadband provider, do not connect this device to any PC or electronic product. Any wrong connection may cause any power or fire risk.
- Do not place this device on an unstable surface or support.

2 Overview

The router is a highly ADSL2/2+ Integrated Access Device and can support ADSL link with downstream up to 24 Mbps and upstream up to 1 Mbps. It is designed to provide a simple and cost-effective ADSL Internet connection for a private Ethernet. The Router combines high-speed ADSL Internet connection, Ethernet uplink and IP routing for the LAN in one package. It is usually preferred to provide high access performance applications for individual users, SOHOs and small enterprises.

The Router is easy to install and use. The Router connects to an Ethernet LAN or computers via standard Ethernet ports, while the ADSL connection is made using an ordinary telephone line with standard connectors. You can connect the Ethernet interface of WAN to Internet with an Ethernet cable for ETH uplink. Multiple workstations can be networked and connected to the Internet via a single Wide Area Network (WAN) interface and a single global IP address. The advanced security enhancements, packet filtering and port redirection help protect your network from potentially malicious devastating intrusions out of your network.

Network and Router management is done through the web-based management interface that can be accessed through the local Ethernet using a web browser. You may also enable remote management to configure the Router via the WAN interface.

2.1 Application

- SOHOs
- Small enterprises
- Higher data rate broadband sharing
- PC file and application sharing
- Network and online gaming

2.2 Features

- User-friendly GUI for web configuration
- Several preconfigured popular games. Enable the game, and the port settings will be automatically configured.

- Compatible with all standard Internet applications
- Industry standard and interoperable ADSL interface
- Simple web-based status page displaying system configuration and linking to configuration pages
- Downloadable flash software updates
- Support utmost 8 permanent virtual circuits (PVC)
- Support utmost 8 PPPoE sessions
- Support RIP v1 & RIP v2
- Optimized Linux 2.6 Operating System
- IP routing and bridging
- Asynchronous transfer mode (ATM) , PTM (Packet Transfer mode) and digital subscriber line (DSL) support
- Ethernet uplink
- Point-to-point protocol (PPP)
- Network/port address translation (NAT/PAT)
- Quality of service (QoS)
- Universal plug-and-play (UPnP)
- File server for network attached storage (NAS) devices
- Web filtering
- Management and control

  Web-based management (WBM)

  Command line interface (CLI)

  TR-069 WAN management protocol
- Remote update
- System statistics and monitoring
- DSL router is targeted at the following platforms: DSL modems and bridge.

2.3 Standards Compatibility and Compliance

- Support application level gateway (ALG)
- ITU G.992.1 (G.dmt)
- ITU G.992.2 (G.lite)
- ITU G.994.1 (G.hs)
- ITU G.992.3 (ADSL2)
- ITU G.992.5 (ADSL2+)

3 Hardware Description and Hardware Installation

✍ **Note:**

The figures in this document are for reference only.

3.1 Hardware Description

3.1.1 Front Panel

Figure 1 Front panel

The following table describes the indicators on the front panel.

Indicator	Color	Status	Description
Power	Green	On	The device is powered on and the device operates normally.
		Blink	The software is upgrading.
		Off	The device is powered off.
	Red	On	The device is initiating.
		Blink	The software is upgrading.
ADSL	Green	On	DSL link has established.
		Blink	The DSL line is training.
		Off	Device is powered off.
Internet	Green	On	The WAN connection is established.
		Blink	Data is being transmitted through the WAN interface.
		Off	The WAN connection is disabled.
	Red	On	PPPoE dialup fails.
LAN 1/2/3/4	Green	On	The Ethernet interface is connected.
		Blink	Data is being transmitted through the Ethernet interface.
		Off	The Ethernet interface is disconnected.

3.1.2 Rear Panel

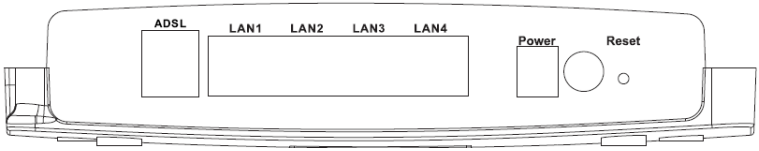


Figure 2 Rear panel

The following table describes the interfaces and buttons on the rear panel.

Interface	Description
ADSL	RJ-11 port: Connect the router to a DSL connector or splitter through a telephone cable.
LAN 1~4	RJ-45 port, for connecting the router to a PC or another network device.
Power	Power interface, for connecting the power adapter.
◯	Power switch.
Reset	Press the button and hold for at least 1 second before releasing it. System restores the factory default settings.

Warning:

*Do not press the **Reset** button unless you want to clear the current settings. The **Reset** button is in a small circular hole on the rear panel. To restore the default settings, please press the **Reset** button gently and hold for 1 second by inserting a fine needle into the hole before releasing the button. The system will reboot and*

return to the factory defaults.

3.2 Hardware Installation

Step 1 Connect the **ADSL** port of the router to the Modem port of the splitter using a telephone cable. Connect the phone to the phone port of the splitter using a telephone cable. Connect the incoming line to the Line port of the splitter.

The spliiter has three ports:

- **LINE**: Connect to a wall phone jack (RJ-11 jack)
- **Modem**: Connect to the ADSL interface of the router
- **PHONE**: Connect to a telephone set

Step 2 Connect the **LAN** port of the router to the network card of the PC through an Ethernet cable.

Step 3 Plug one end of the power adapter into the wall outlet and the other end to the **Power** port of the router.

The following figure shows the connection of the DSL router, PC and telephones.

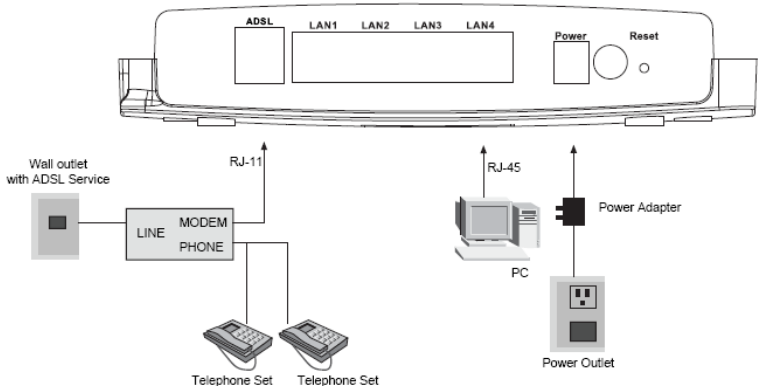


Figure 3 Connecting the DSL router

4 PC Network Configuration and Login

4.1 PC Network Configuration

Each network interface on the PC should either be configured with a statically
defined IP address and DNS address, or be instructed to automatically obtain an IP address using the network DHCP server. DSL router provides a DHCP server on its LAN and it is recommended to configure your LAN to automatically obtain its IP address and DNS server IP address.

The configuration principle is identical but should be carried out differently on each operating system.

The following displays the **TCP/IP Properties** dialog box on Windows XP.

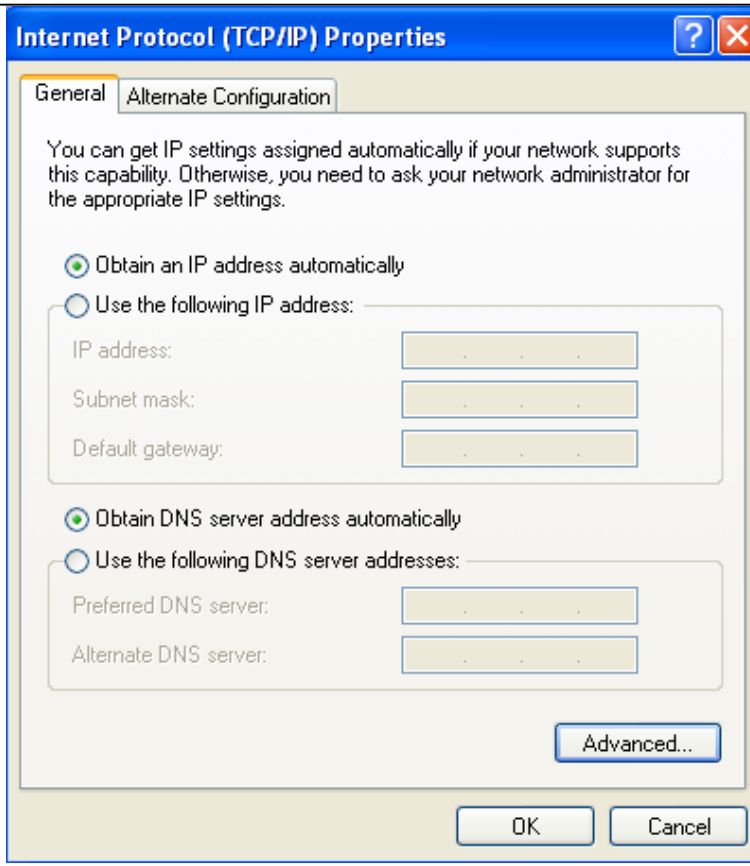

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 4 IP and DNS configuration

TCP/IP configuration steps for Windows XP are as follows:

Step 1 Choose Start > Control Panel > Network Connections.

Step 2 Right-click the Ethernet connection icon and choose **Properties**.

Step 3 On the **General** tab, select the **Internet Protocol (TCP/IP)** component and click Properties.

Step 4 The **Internet Protocol (TCP/IP) Properties** window appears.

Step 5 Select the **Obtain an IP address automatically** radio button.

Step 6 Select the **Obtain DNS server address automatically** radio button.

Step 7 Click **OK** to save the settings.

4.2 Logging in to the DSL Router

To log in to the DSL router, perform the followings:

Step 1 Open a Web browser on your computer.

Step 2 Enter ***http://192.168.1.1*** (the default IP address of the DSL router) in the address bar. The login page appears.

Step 3 Enter the user name and the password. The default username and password of the super user are **admin** and **admin**. The username and password of the common user are **user** and **user**. You need not enter the username and the password again if you select the option

Remember my password. It is recommended to change these default values after logging in to the DSL router for the first time.

Step 4 Click **OK** to log in to the Web page. Otherwise, please click **Cancel** to exit the login page.

Figure 5 Login page

After logging in to the DSL router as a super user, you can query, configure, and modify all the settings, and diagnose the system.

5 Web-Based Management

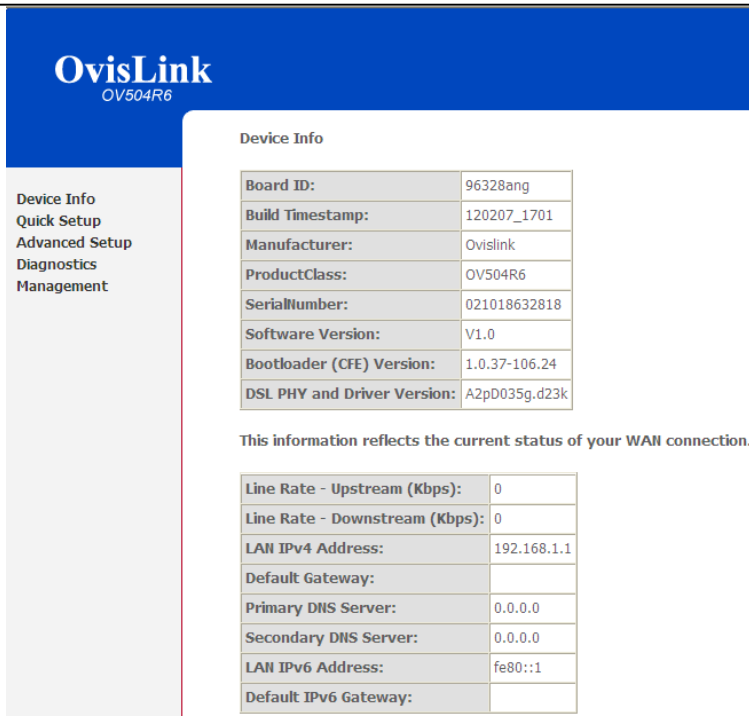
This chapter describes how to use Web-based management of the DSL router,
which allows you to configure and control all DSL router features and system parameters in a user-friendly GUI.

5.1 Device Information

Choose **Device Info**, and the submenus of **Device Info** include **Summary**, **WAN**, **Statistics**, **Route**, **ARP and DHCP**.

5.1.1 Summary

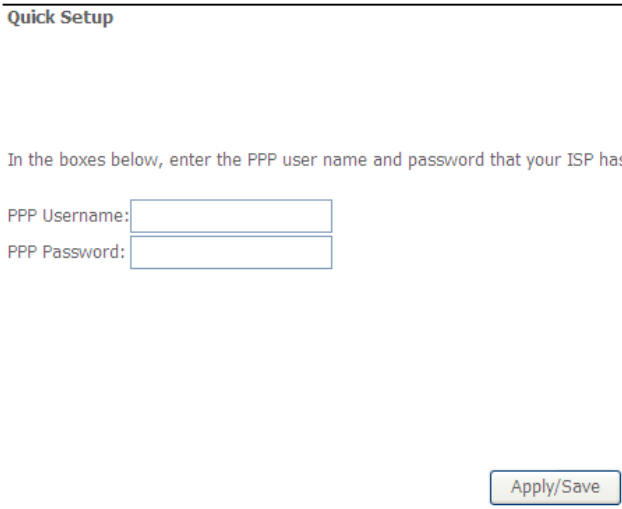
Choose **Device Info > Summary**, and the following page appears.



This page displays the device information such as the board ID, software version, and the information of your WAN connection including the upstream rate and the LAN address.

5.2 Quick Setup

Choose **Quick Setup**, and the following page appears.


Quick Setup
In the boxes below, enter the PPP user name and password that your ISP has provided to you.
PPP Username:
PPP Password:
Apply/Save

After configuring a PVC of PPPoE type and connecting the ADSL line to the router, input the username and password to access the Internet.

5.3 Advanced Setup

Choose **Advanced Setup** and the submenus include **Layer2 Interface**, **WAN Service**, **LAN**, **NAT**, **Security**, **Parental Contorl**, **Quality of Service**, **Routing**,
DSL, **UpnP**, **DNS Proxy**, **Print Server**, **Packet Acceleration**, **Storage Service**, **Interface Grouping**, **IPSec**, **Certificate**, **Power Management** and **Multicast**.

5.3.1 Layer2 Interface

ATM Interface

Choose **Advanced Setup** > **Layer2 Interface** > **ATM Interface** , and the following page appears.

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
atm0	0	33	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	☐
atm1	0	35	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	☐
atm2	8	35	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	☐

Add Remove

Figure 6 DSL ATM interface configuration

In this page, you can add or remove the DSL ATM Interfaces.

Click the **Add** button to display the following page.

ATM PVC Configuration

This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

VPI: [0-255] 0

VCI: [32-65535] 35

Select DSL Latency

☑ Path0

☐ Path1

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

◉ EoA

○ PPPoA

○ IPoA

Select Connection Mode

◉ Default Mode - Single service over one connection

○ VLAN MUX Mode - Multiple Vlan service over one connection

Encapsulation Mode: LLC/SNAP-BRIDGING

Service Category: UBR Without PCR

Select IP QoS Scheduler Algorithm

◉ Strict Priority

Precedence of the default queue: 8 (lowest)

○ Weighted Fair Queuing

Weight Value of the default queue: [1-63] 1

MPAAL Group Precedence: 8

Back Apply/Save

Figure 7 ATM PVC configuration

In this page, you can set the VPI and VCI values, and select the DSL latency, link type (EoA is for PPPoE, IPoE and Bridge.), connection mode, encapsulation mode, service category, and IP QoS scheduler algorithm.

- **VPI (Virtual Path Identifier)**: The virtual path between two points in an ATM network, and its valid value is from 0 to 255.
- **VCI (Virtual Channel Identifier)**: The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols).
- **Select DSL Latency**: You may select **Path0** or **Path1**.
- **Select DSL Link Type**: You may select **EoA** (for PPPoE, IPoE and Bridge), **PPPoA** or **IPoA**.
- **Select Connection Mode:** You may select the **Default Mode** or the **VLAN MUX Mode**.
- **Encapsulation Mode**: You may select **LLC/SNAP-BRIDGING** or **VC/MUX** in the drop-down list.
- **Service Category:** you may select **UBR Without PCR**, **UBR With PCR**, **CBR**, **Non Realtime VBR** or **Realtime VBR** from the drop-down lsit.
- **Select IP QoS Scheduler Algorithm:** You may select **Strict Priority** and **Weighted Fair Queuing**.

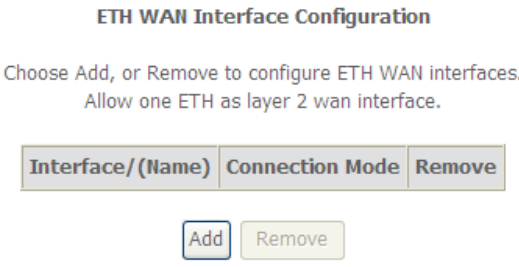
Note:

QoS cannot be set for CBR and Realtime VBR.

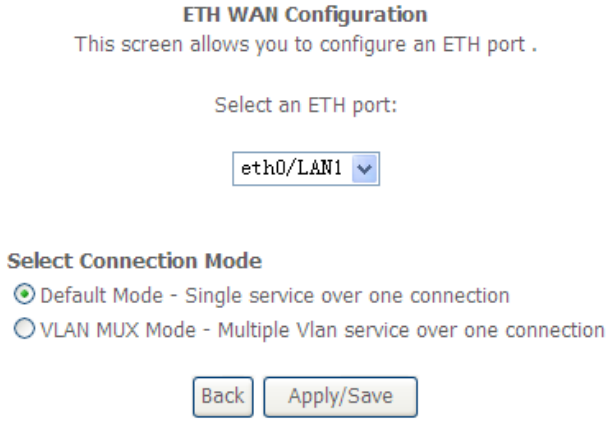
After finishing setting, click the **Apply/Save** button to enable the settings.

ETH Interface

Choose **Advanced Setup** > **Layer2 Interface** > **ETH Interface**, and the following page appears.



In this page, you can add or remove the DSL ETH Interfaces.
Click the **Add** button to display the following page.


ETH WAN Configuration
This screen allows you to configure an ETH port .
Select an ETH port:
eth0/LAN1
Select Connection Mode
Default Mode - Single service over one connection
VLAN MUX Mode - Multiple Vlan service over one connection
Back
Apply/Save

- **Select an ETH port**: You can select it from the drop-down list, such as eth1/eth1.
- **Select Connection Mode**
  - **Default Mode** – Single service over one connection.
  - **VLAN MUX Mode** – Multiple Vlan service over one connection.

After finishing setting, click the **Apply/Save** button to enable the settings.

5.3.2 WAN Service

Choose **Advance Setup** > **WAN Service**, and the following page appears.

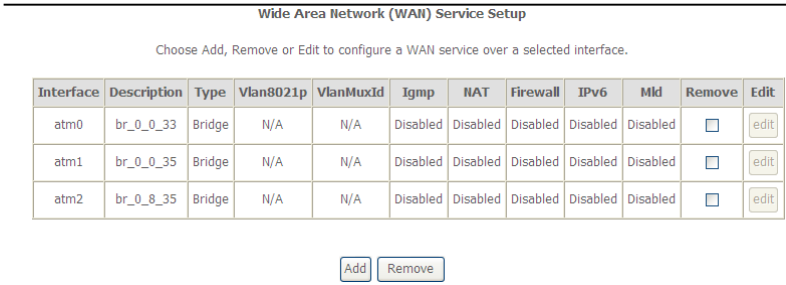

Wide Area Network (WAN) Service Setup
Choose Add, Remove or Edit to configure a WAN service over a selected interface.
Interface Description Type Vlan8021p VlanMuxId Igmp NAT Firewall IPv6 Mld Remove Edit
atm0 br_0_0_33 Bridge N/A N/A Disabled Disabled Disabled Disabled Disabled edit
atm1 br_0_0_35 Bridge N/A N/A Disabled Disabled Disabled Disabled Disabled edit
atm2 br_0_8_35 Bridge N/A N/A Disabled Disabled Disabled Disabled Disabled edit
Add
Remove

Figure 8 WAN service configuration

In this page, you may add, remove or edit a WAN service.

5.3.2.1 Adding a PPPoE WAN Service

This section describes the steps for adding the PPPoE WAN service.

Step1 In the **Wide Area Network (WAN) Service Setup** page, click the **Add** button to display the following page. (First a proper ATM configuration should be added for this WAN service.)

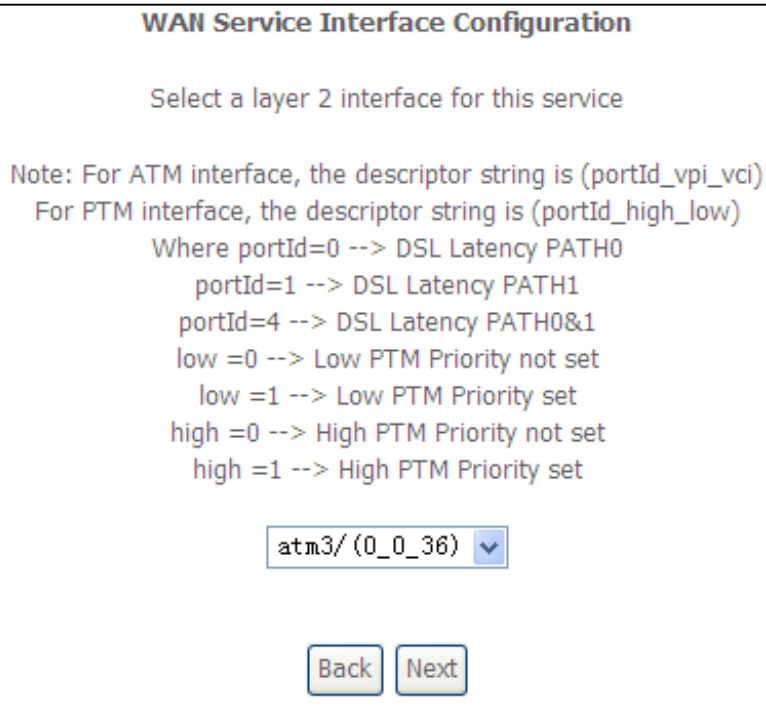

WAN Service Interface Configuration
Select a layer 2 interface for this service
Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set
atm3/(0_0_36)
Back
Next

Figure 9 WAN service interface configuration (PPPoE)

Step2 In this page, you can select an ATM Interface for the WAN service. After selecting the ATM interface, click **Next** to display the following page.

Figure 10 WAN service configuration (PPPoE)

Step3 In this page, select the WAN service type to be **PPP over Ethernet (PPPoE)**. You may also select Enable IPv6 for this service. Click **Next** to display the following page.

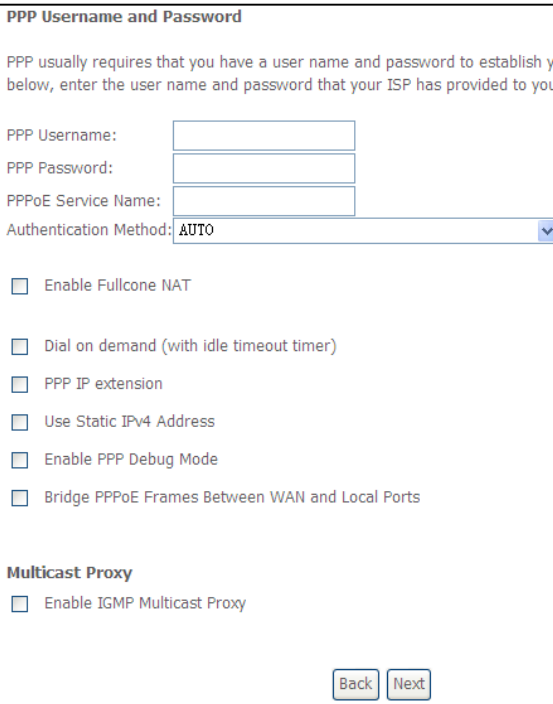

PPP Username and Password
PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.
PPP Username:
PPP Password:
PPPoE Service Name:
Authentication Method:
AUTO
Enable Fullcone NAT
Dial on demand (with idle timeout timer)
PPP IP extension
Use Static IPv4 Address
Enable PPP Debug Mode
Bridge PPPoE Frames Between WAN and Local Ports
Multicast Proxy
Enable IGMP Multicast Proxy
Back
Next

Figure 11 PPP username and password (PPPoE)

Step4 In this page, you can modify the PPP username, PPP password, PPPoE service name and authentication method.

- **PPP Username:** The correct user name provided by your ISP.
- **PPP Password:** The correct password provided by your ISP.
- **PPPoE Service Name:** If your ISP provides it to you, please enter it. If not, do not enter any information.
- **Authentication Method:** The value can be AUTO, PAP, CHAP, or MSCHAP. Usually, you can select AUTO.
- **Enable Fullcone NAT:** NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

- **Dial on demand (with idle timeout timer):** If this function is enabled, you need to enter the idle timeout time. Within the preset minutes, if the modem does not detect the flow of the user continuously, the modem automatically stops the PPPoE connection. Once it detects the flow (like access to a webpage), the modem restarts the PPPoE dialup. If this function is disabled, the modem performs PPPoE dial-up all the time. The PPPoE connnection does not stop, unless the modem is powered off and DSLAM or uplink equipment is abnormal.
- **PPP IP extension:** If you want to configure DMZ Host, you should enable it first.
- **Use Static IPv4 Address:** If this function is disabled, the modem obtains an IP address assigned by an uplink equipment such as BAS, through PPPoE dial-up. If this function is enabled, the modem uses this IP address as the WAN IP address.
- **Enable PPP Debug Mode:** Enable or disable this function.
- **Bridge PPPoE Frames Between WAN and Local Ports:** Enable or disable this function.
- **Enable IGMP Multicast Proxy:** If you want PPPoE mode to support IPTV, enable it.

Step5 After setting the parameters, click **Next** to display the following page.

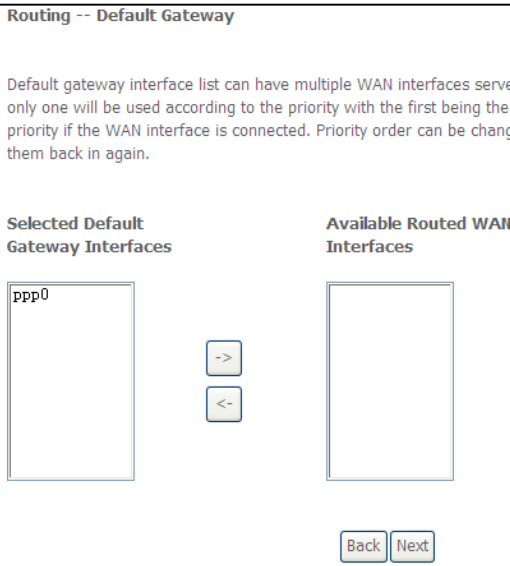

Routing -- Default Gateway
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Selected Default Gateway Interfaces
Available Routed WAN Interfaces
ppp0
->
<-
Back
Next

Figure 12 Routing-default gateway (PPPoE)

Step6 In this page, select a preferred WAN interface as the system default gateway interface and then click **Next** to display the following page.

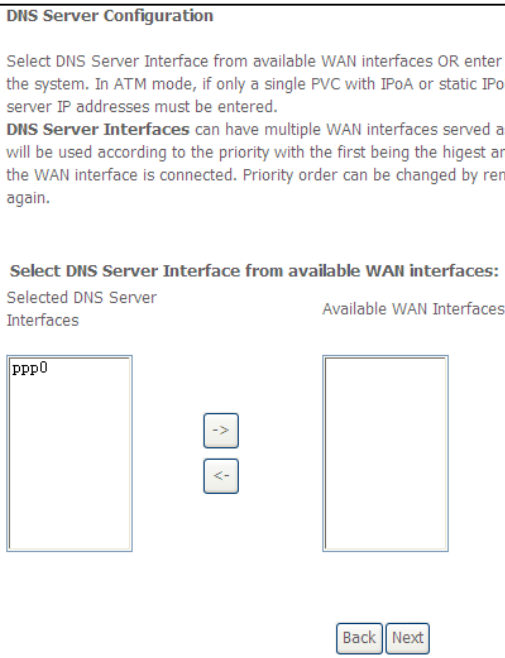

DNS Server Configuration
Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Select DNS Server Interface from available WAN interfaces:
Selected DNS Server Interfaces
Available WAN Interfaces
ppp0
->
<-
Back
Next

Figure 13 DNS server configuration (PPPoE)

Step7 In this page, you may select a DNS server interface from the available WAN interfaces. Click **Next**, and the following page appears.

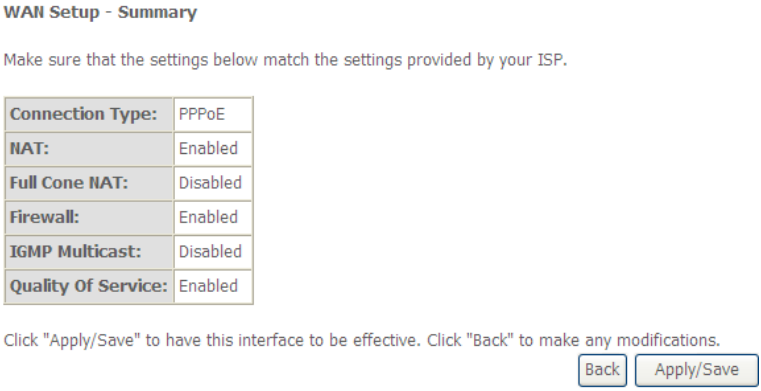

WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
Connection Type: PPPoE
NAT: Enabled
Full Cone NAT: Disabled
Firewall: Enabled
IGMP Multicast: Disabled
Quality Of Service: Enabled
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.
Back
Apply/Save

Figure 14 PPPoE summary

Step8 In this page, it displays the information about the PPPoE settngs. Click **Apply/Save** to save and apply the settings.

5.3.2.2 Adding a MER (IPoE) WAN service

This section describes the steps for adding the MER WAN service.

Step1 In the **Wide Area Network (WAN) Service Setup** page, click the **Add** button to display the following page. (At first, you must add a ATM configuration for this WAN service.)

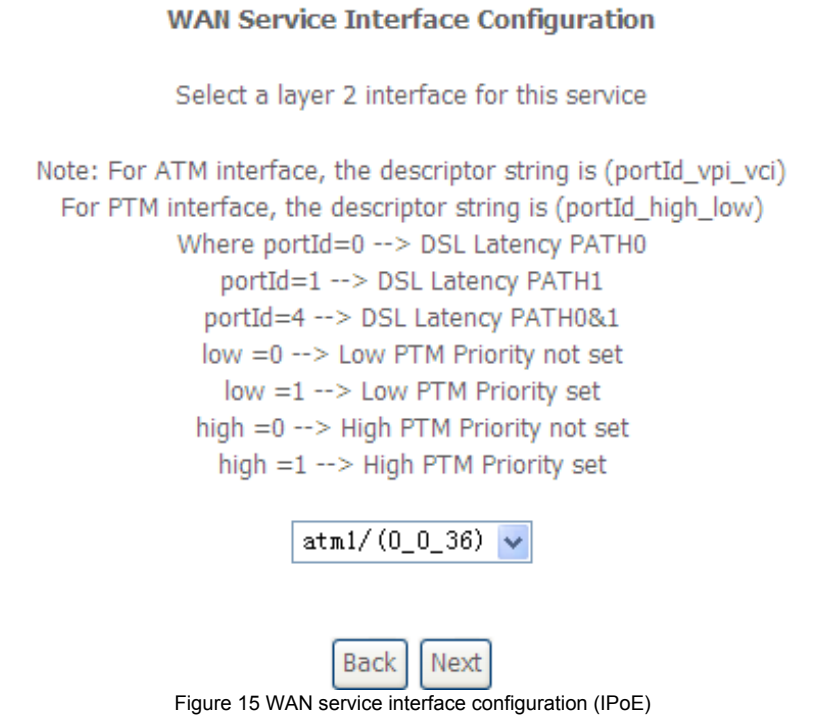

WAN Service Interface Configuration
Select a layer 2 interface for this service
Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set
atm1/(0_0_36)
Back
Next

Figure 15 WAN service interface configuration (IPoE)

Step2 Select an ATM Interface, and then click **Next** to display the following page.

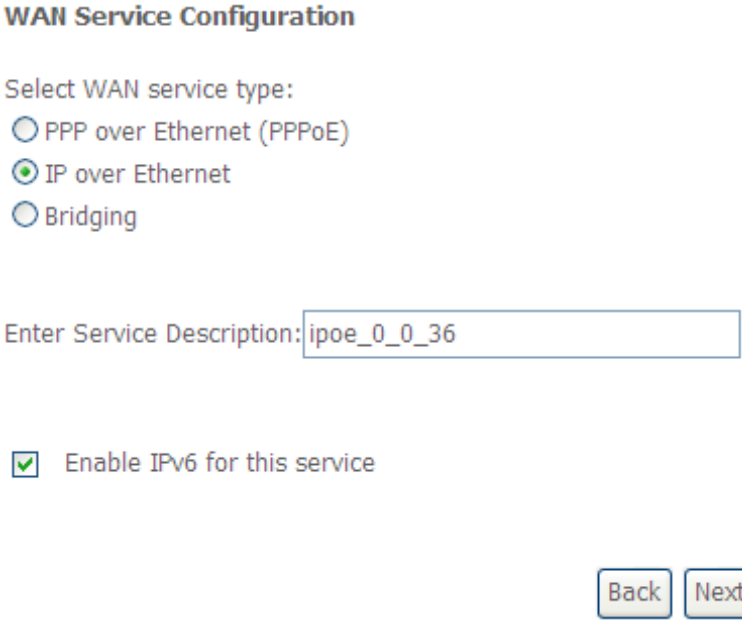


Figure 16 WAN service configuration (IPoE)

Step3 In this page, select the WAN service type to be IP over Ethernet, enter the service description for this service, and you may also enable IPv6 for this service. After finishing setting, click **Next** to display the following page.

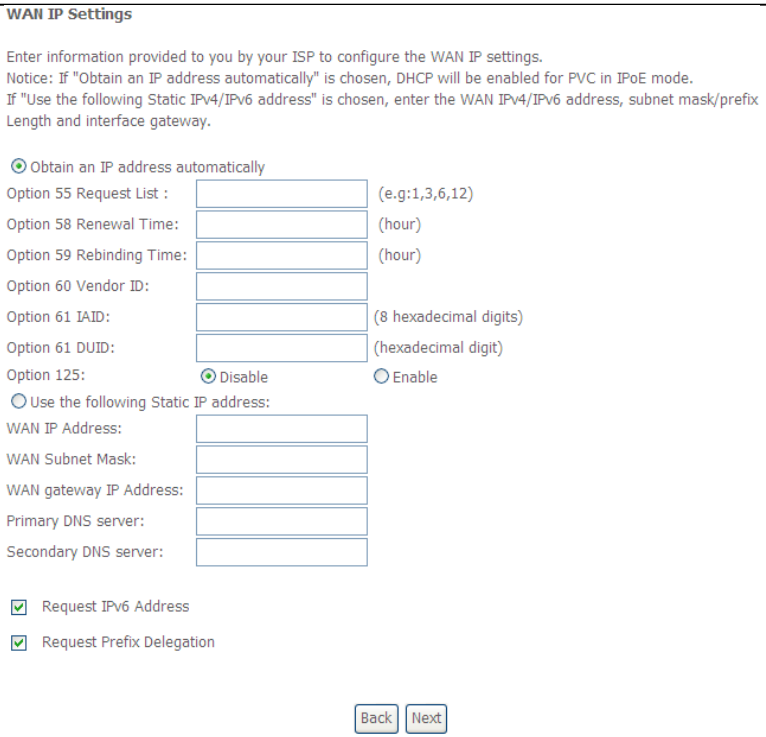

WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.
If "Use the following Static IPv4/IPv6 address" is chosen, enter the WAN IPv4/IPv6 address, subnet mask/prefix Length and interface gateway.
Obtain an IP address automatically
Option 55 Request List :
(e.g:1,3,6,12)
Option 58 Renewal Time:
(hour)
Option 59 Rebinding Time:
(hour)
Option 60 Vendor ID:
Option 61 IAID:
(8 hexadecimal digits)
Option 61 DUID:
(hexadecimal digit)
Option 125:
Disable
Enable
Use the following Static IP address:
WAN IP Address:
WAN Subnet Mask:
WAN gateway IP Address:
Primary DNS server:
Secondary DNS server:
Request IPv6 Address
Request Prefix Delegation
Back
Next

Figure 17 WAN IP settings (IPoE)

- **Request IPv6 Address:** Select it to obtain IP addresses of IPv6 type.
- **Request Prefix Delegation:** Select it to obtain IPv6 prefix. An IPv6 prefix is equivalent an IPv4 subnet mask.

✍ **Note:**

When IPv6 is enabled, you are suggested to keep the default options here.

Step4 In this page, you may modify the WAN IP settings. You may select obtain an IP address automatically or manually enter the IP address provided by your ISP. Click **Next** and the following page appears.

✍ **Note:**

If **Obtain an IP address automatically** is selected, DHCP will be enabled for PVC in MER mode. If **Use the following Static IP address** is selected, enter the WAN IP address, subnet mask, gateway IP address, and primary and

secondary DNS servers.

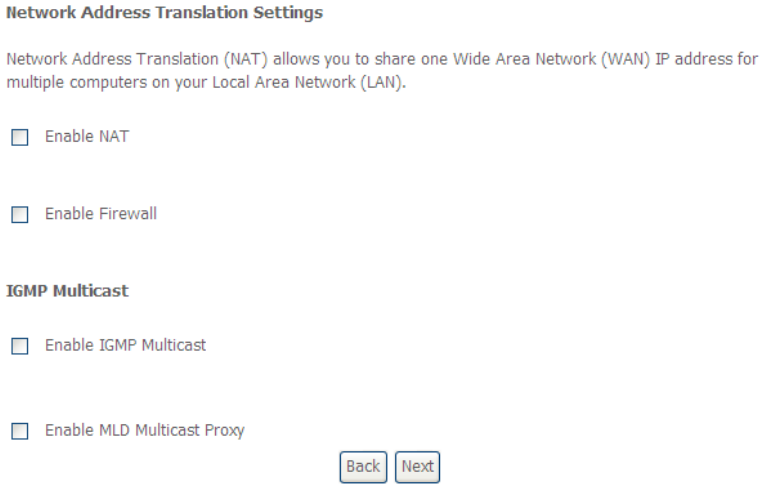

Network Address Translation Settings
Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).
Enable NAT
Enable Firewall
IGMP Multicast
Enable IGMP Multicast
Enable MLD Multicast Proxy
Back
Next

Figure 18 Network address translation settings (IPoE)

Step5 In this page, you can set the network address translation settings,for example, enabling NAT, firewall, IGMP multicast and MLD multicast proxy. After finishing setting, click **Next** and the following page appears.

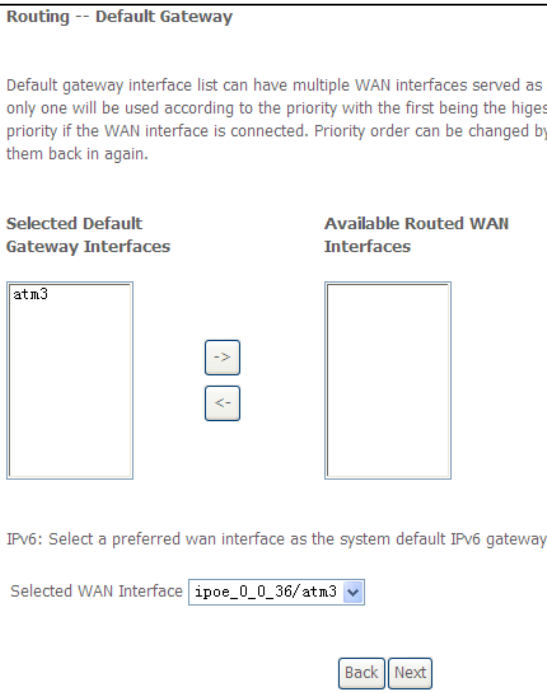

Routing -- Default Gateway
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Selected Default Gateway Interfaces
Available Routed WAN Interfaces
atm3
->
<-
IPv6: Select a preferred wan interface as the system default IPv6 gateway.
Selected WAN Interface
ipoe_0_0_36/atm3
Back
Next

Figure 19 Routing-default gateway (IPoE)

Step6 In this page, select a preferred WAN interface as the system default gateway interface, select a WAN interface as the system default IPv6 gateway, and then click **Next** to display the following page.

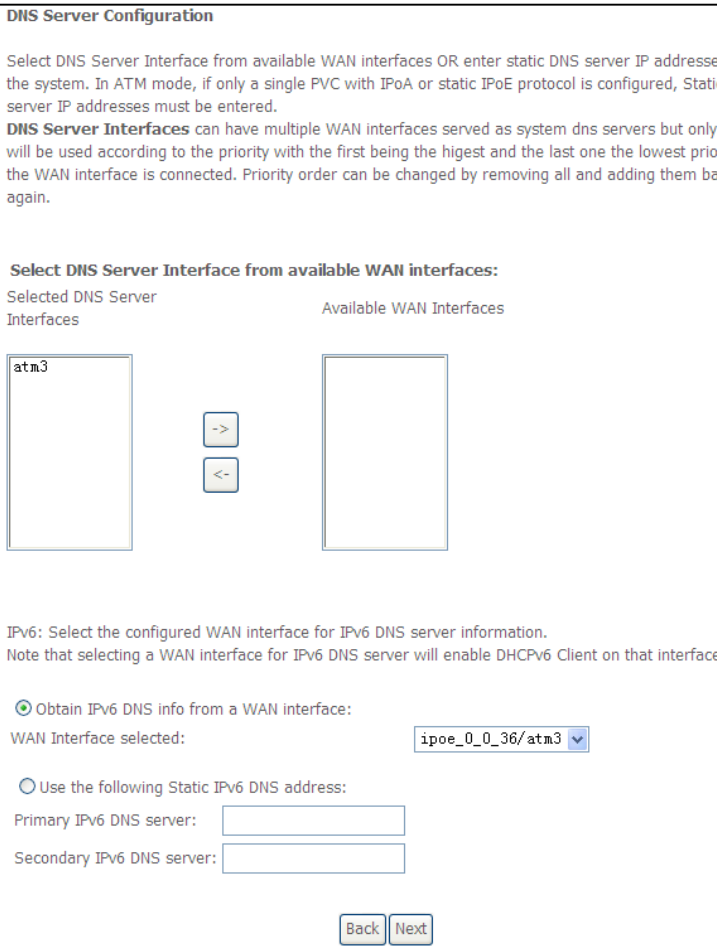

DNS Server Configuration
Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Select DNS Server Interface from available WAN interfaces:
Selected DNS Server Interfaces
Available WAN Interfaces
atm3
->
<-
IPv6: Select the configured WAN interface for IPv6 DNS server information.
Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.
Obtain IPv6 DNS info from a WAN interface:
WAN Interface selected:
ipoe_0_0_36/atm3
Use the following Static IPv6 DNS address:
Primary IPv6 DNS server:
Secondary IPv6 DNS server:
Back
Next

Figure 20 DNS server configuration (IPoE)

Step7 In this page, you may select a DNS server interface from the available WAN interfaces. After finishing setting, click **Next** to display the following page.

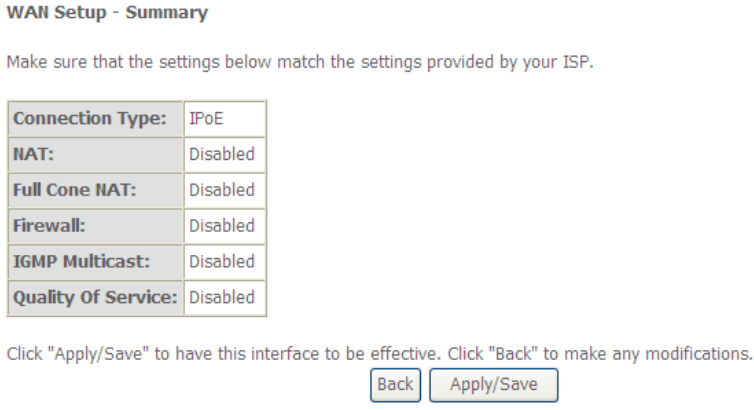

WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
Connection Type: IPoE
NAT: Disabled
Full Cone NAT: Disabled
Firewall: Disabled
IGMP Multicast: Disabled
Quality Of Service: Disabled
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.
Back
Apply/Save

Figure 21 IPoE summary

Step8 In this page, it displays the information about the IPoE settngs.Click **Apply/Save** to save and apply the settings.

5.3.2.3 Adding a PPPoA WAN service

This section describes the steps for adding the PPPoA WAN service.

Step1 Choose **Advanced Setup** > **Layer2 Interface** > **ATM Interface** to dsipaly the **DSL ATM Interface Configuration** page. In this page, you need to add a PVC for PPPoA mode. Click the **Add** button in the **DSL ATM Interface Configuration** page to display the following page.

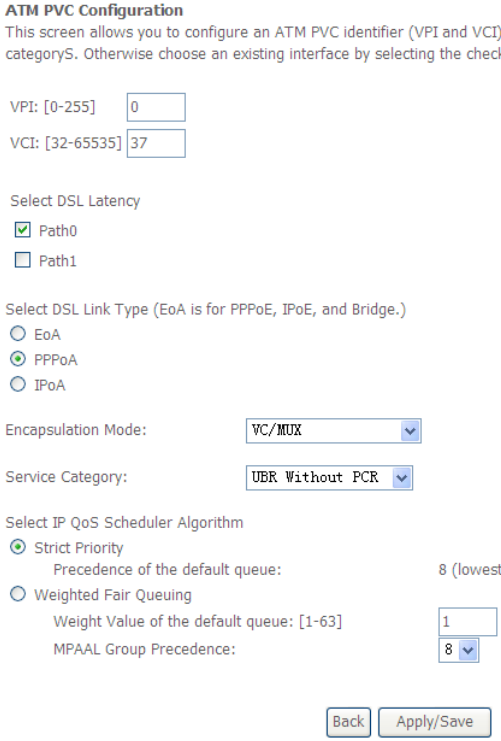

ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service categoryS. Otherwise choose an existing interface by selecting the checkbox to enable it.
VPI: [0-255] 0
VCI: [32-65535] 37
Select DSL Latency
Path0
Path1
Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)
EoA
PPPoA
IPoA
Encapsulation Mode: VC/MUX
Service Category: UBR Without PCR
Select IP QoS Scheduler Algorithm
Strict Priority
Precedence of the default queue: 8 (lowest)
Weighted Fair Queuing
Weight Value of the default queue: [1-63] 1
MPAAL Group Precedence: 8
Back
Apply/Save

Figure 22 ATM PVC configuration (PPPoA)

Step2 Select the DSL link type to be **PPPoA**, and select the encapsulation mode to be **VC/MUX** (according to the uplink equipment). After finishing setting, click the **Apply/Save** button to apply the settings.

Step3 Choose **WAN Service** and click **Add** to display the following page.

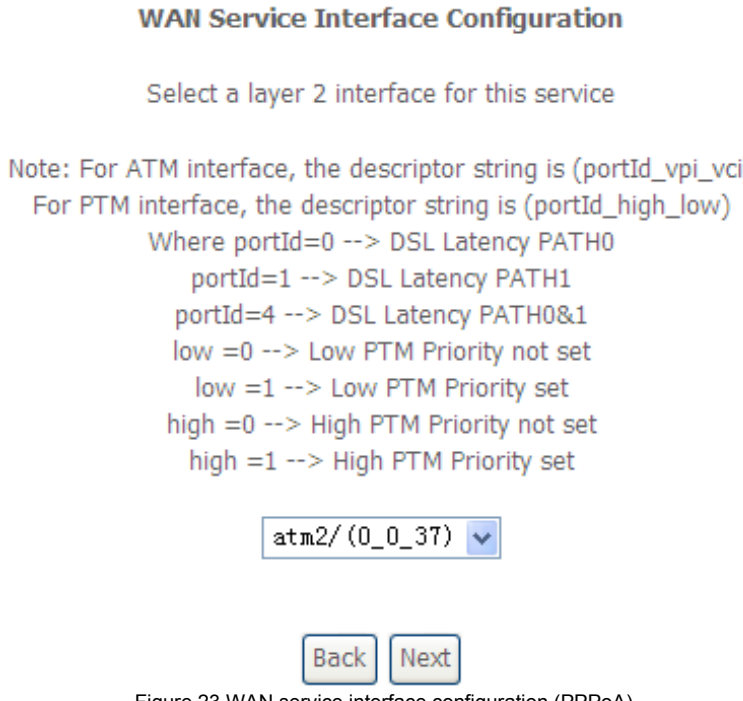

WAN Service Interface Configuration
Select a layer 2 interface for this service
Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set
atm2/(0_0_37)
Back
Next

Figure 23 WAN service interface configuration (PPPoA)

Step4 Select the proper interface for the WAN service, and then click **Next** to display the following page.

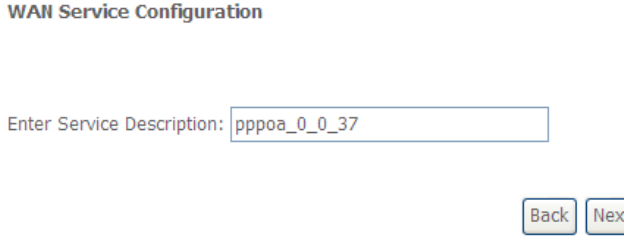


Figure 24 WAN service configuration (PPPoA)

Step5 In this page, you may modify the service description. Click **Next** to display the following page.

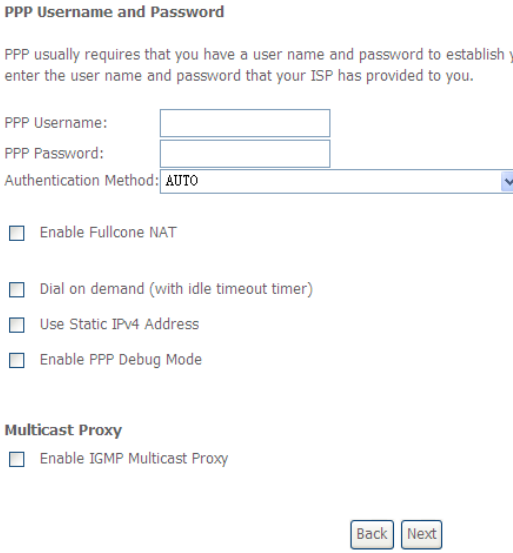

PPP Username and Password
PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.
PPP Username:
PPP Password:
Authentication Method:
AUTO
Enable Fullcone NAT
Dial on demand (with idle timeout timer)
Use Static IPv4 Address
Enable PPP Debug Mode
Multicast Proxy
Enable IGMP Multicast Proxy
Back
Next

Figure 25 PPP username and password (PPPoA)

- **PPP Username:** The correct user name provided by your ISP.
- **PPP Password:** The correct password provided by your ISP.
- **Authentication Method:** The value can be AUTO, PAP, CHAP, or MSCHAP. Usually, you can select AUTO.
- **Enable Fullcone NAT:**. NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.
- **Dial on demand (with idle timeout timer):** If this function is enabled, you need to enter the idle timeout time. Within the preset minutes, if the modem does not detect the flow of the user continuously, the modem automatically stops the PPPoA connection. Once it detects the flow (like access to a webpage), the modem restarts the PPPoA dialup. If this function is disabled, the modem performs PPPoA dial-up all the time. The PPPoA connnection

does not stop, unless the modem is powered off and DSLAM or uplink equipment is abnormal.

- **Use Static IPv4 Address:** If this function is disabled, the modem obtains an IP address assigned by an uplink equipment such as BAS, through PPPoA dial-up. If this function is enabled, the modem uses this IP address as the WAN IP address.
- **Enable PPP Debug Mode:**Enable or disable this function.
- **Enable IGMP Multicast Proxy:** If you want PPPoE mode to support IPTV, enable it.

Step6 In this page, enter the PPP username and PPP password provided by your ISP. Select the authentication method according to your requirement. After finishing setting, click **Next** to display the following page.

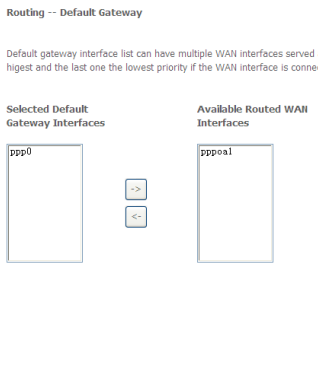

Routing -- Default Gateway
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Selected Default Gateway Interfaces
Available Routed WAN Interfaces
ppp0
pppoa1
->
<-
Back
Next

Figure 26 Routing-default gateway (PPPoA)

Step7 In this page, select a preferred WAN interface as the system default gateway interface and then click **Next** to display the following page.

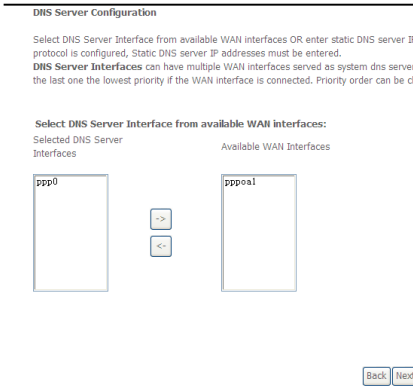

DNS Server Configuration
Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Select DNS Server Interface from available WAN interfaces:
Selected DNS Server Interfaces
Available WAN Interfaces
ppp0
->
<-
pppoal
Back
Next

Figure 27 DNS server configuration (PPPoA)

Step8 In this page, you may select a DNS server interface from the available WAN interfaces. After finishing setting, click **Next** to display the following page.

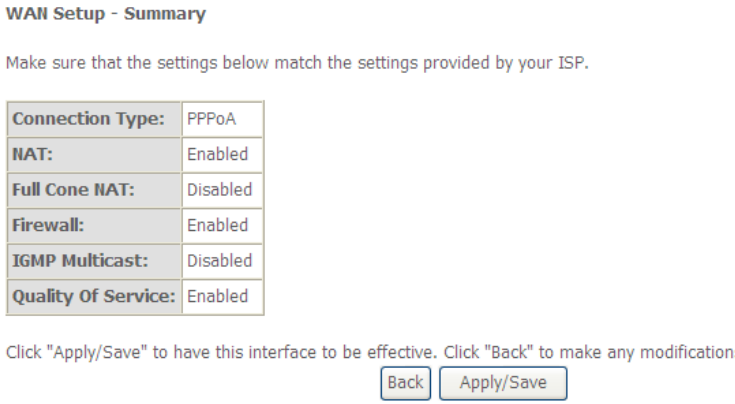

WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
Connection Type: PPPoA
NAT: Enabled
Full Cone NAT: Disabled
Firewall: Enabled
IGMP Multicast: Disabled
Quality Of Service: Enabled
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.
Back
Apply/Save

Figure 28 PPPoA summary

Step9 In this page, it displays the information about the PPPoA settngs.Click **Apply/Save** to apply the settings. You can modify the settings by clicking the **Back** button if necessary.

5.3.2.4 Adding an IPoA WAN service

This section describes the steps for adding the IPoA WAN service.

Step1 Choose **Advanced Setup > Layer2 Interface > ATM Interface** to dsipaly the **DSL ATM Interface Configuration** page. In this page, you need to add a PVC for IPoA mode. Click the **Add** button in the **DSL ATM Interface Configuration** page to display the following page.

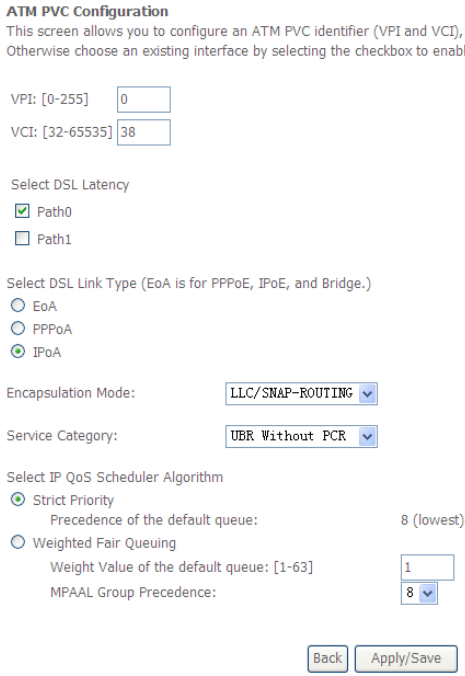

ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service categoryS. Otherwise choose an existing interface by selecting the checkbox to enable it.
VPI: [0-255] 0
VCI: [32-65535] 38
Select DSL Latency
Path0
Path1
Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)
EoA
PPPoA
IPoA
Encapsulation Mode: LLC/SNAP-ROUTING
Service Category: UBR Without PCR
Select IP QoS Scheduler Algorithm
Strict Priority
Precedence of the default queue: 8 (lowest)
Weighted Fair Queuing
Weight Value of the default queue: [1-63] 1
MPAAL Group Precedence: 8
Back
Apply/Save

Figure 29 ATM PVC configuration (IPoA)

Step2 Select the DSL link type to be **IPoA**, and select the encapsulation mode to be **LLC/SNAP-ROUTING** (according to the uplink equipment). After finishing setting, click the **Apply/Save** button to save the settings.

Step3 Choose **WAN Service** and click **Add** to display the following page.

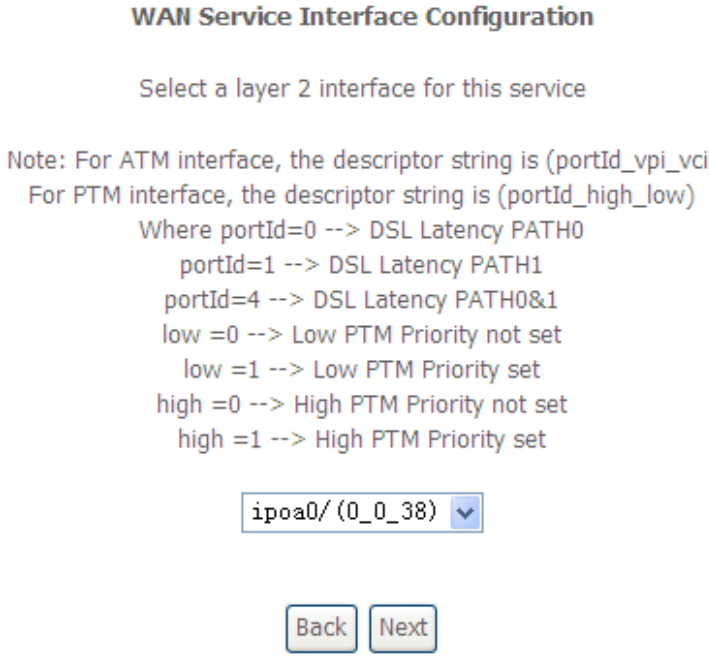

WAN Service Interface Configuration
Select a layer 2 interface for this service
Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set
ipoa0/(0_0_38)
Back
Next

Figure 30 WAN service interface configuration (IPoA)

Step4 Select the proper interface for the WAN service ,and then click **Next** to display the following page.

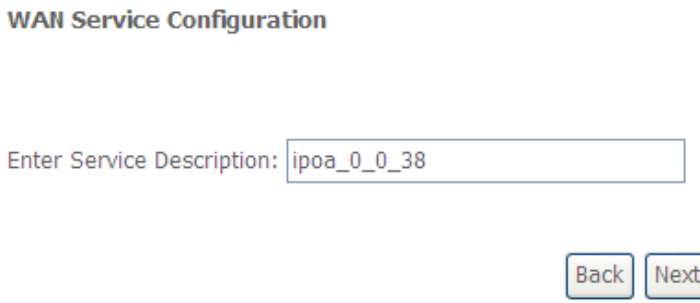


Figure 31 WAN service configuration (IPoA)

Step5 In this page, you may modify the service description. Click **Next** to display the following page.

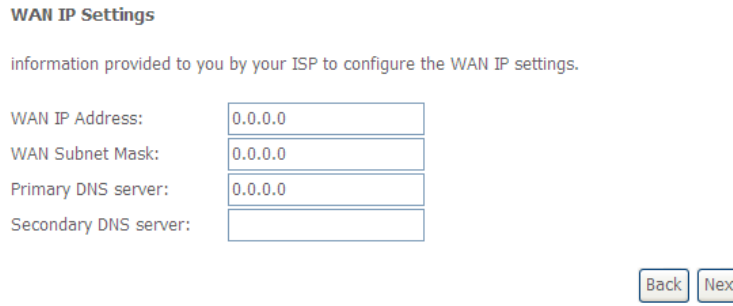


Figure 32 WAN IP settings (IPoA)

Step6 In this page, enter the WAN IP address and the WAN subnet mask provided by your ISP and then click **Next** to display the following page.

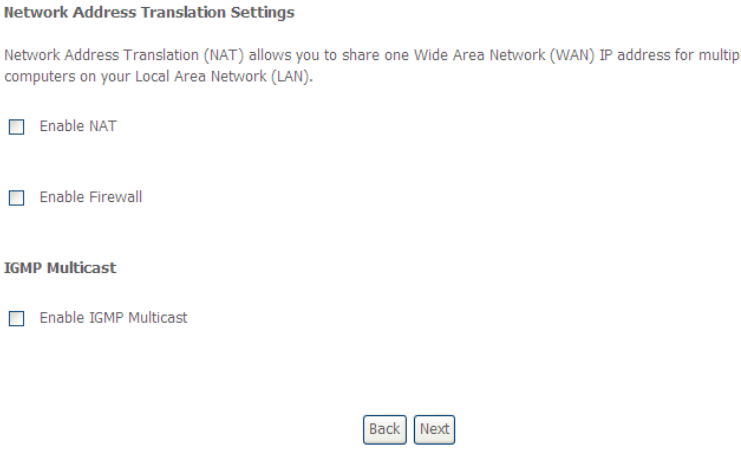

Network Address Translation Settings
Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).
Enable NAT
Enable Firewall
IGMP Multicast
Enable IGMP Multicast
Back
Next

Figure 33 Network address translation settings (IPoA)

In this page, Network Address Translation (NAT) allows you to share one Wide
Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

If you do not want to enable NAT, and wish the user of modem to access the
Internet normally, you need to add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, please enable the NAT function.

Step7 After finishing setting, click **Next** to display the following page.

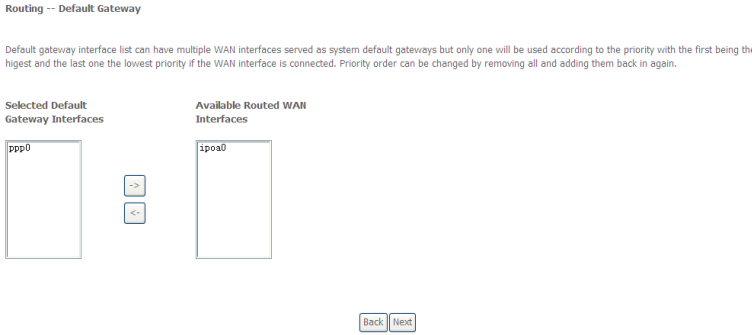

Routing -- Default Gateway
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Selected Default Gateway Interfaces
Available Routed WAN Interfaces
ppp0
ipoa0
->
<-
Back
Next

Figure 34 Routing-default gateway (IPoA)

Step8 In this page, select a preferred WAN interface as the system default gateway interface and then click **Next** to display the following page.

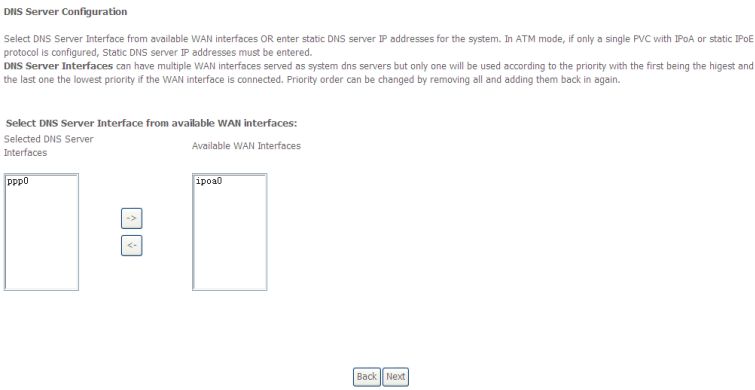

DNS Server Configuration
Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Select DNS Server Interface from available WAN interfaces:
Selected DNS Server Interfaces
Available WAN Interfaces
ppp0
ipoa0
->
<-
Back
Next

Figure 35 DNS server configuration (IPoA)

Step9 In this page, you may select a DNS server interface from the available WAN interfaces. Click **Next** to display the following page.

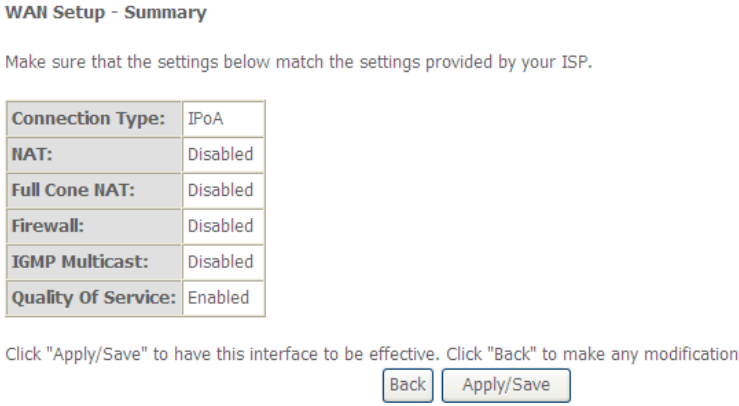

WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
Connection Type: IPoA
NAT: Disabled
Full Cone NAT: Disabled
Firewall: Disabled
IGMP Multicast: Disabled
Quality Of Service: Enabled
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.
Back
Apply/Save

Figure 36 IPoA summary

Step10 In this page, it displays the information about the IPoA settngs. Click **Apply/Save** to save and apply the settings. You can modify the settings by clicking the **Back** button if necessary.

5.3.2.5 Adding a Bridge WAN service

This section describes the steps for adding the Bridge WAN service.

Step1 In the **Wide Area Network (WAN) Service Setup** page, click the **Add** button to display the following page. (At first, you must add a proper ATM configuration for this WAN service.) Click the **Add** button to display the following page.

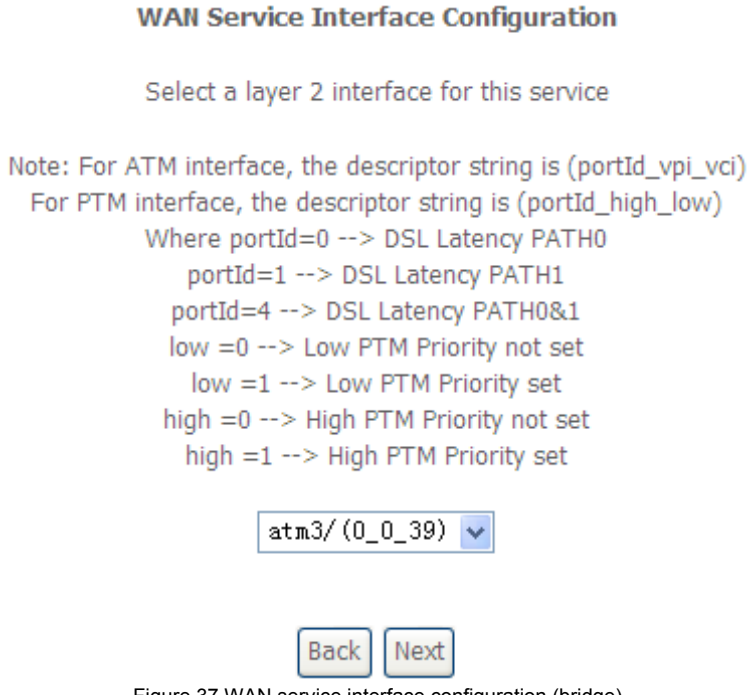

WAN Service Interface Configuration
Select a layer 2 interface for this service
Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set
atm3/(0_0_39)
Back
Next

Figure 37 WAN service interface configuration (bridge)

Step2 Select the proper ATM Interface and then click **Next** to display the following page.

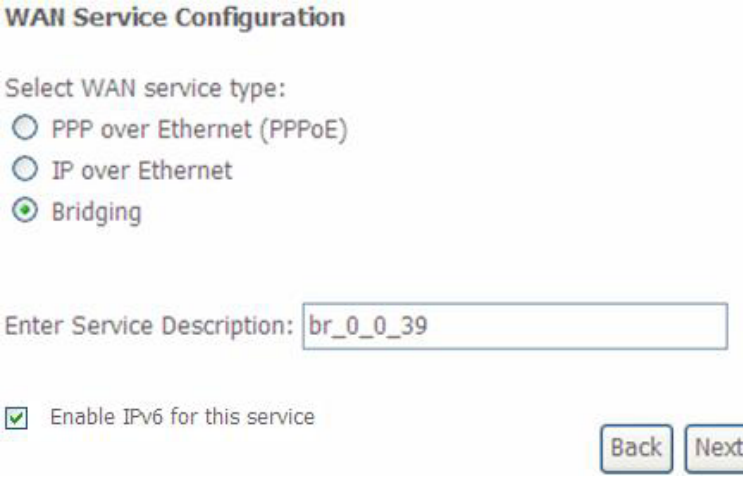


Figure 38 WAN service configuration (bridge)

Step3 In this page, you can select the WAN service type, and modify the service description for this service. After finishing setting, click **Next** to display the following page.

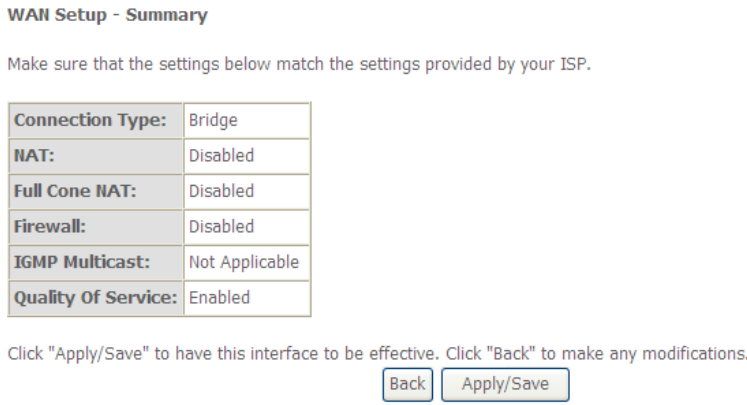

WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
Connection Type: Bridge
NAT: Disabled
Full Cone NAT: Disabled
Firewall: Disabled
IGMP Multicast: Not Applicable
Quality Of Service: Enabled
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.
Back
Apply/Save

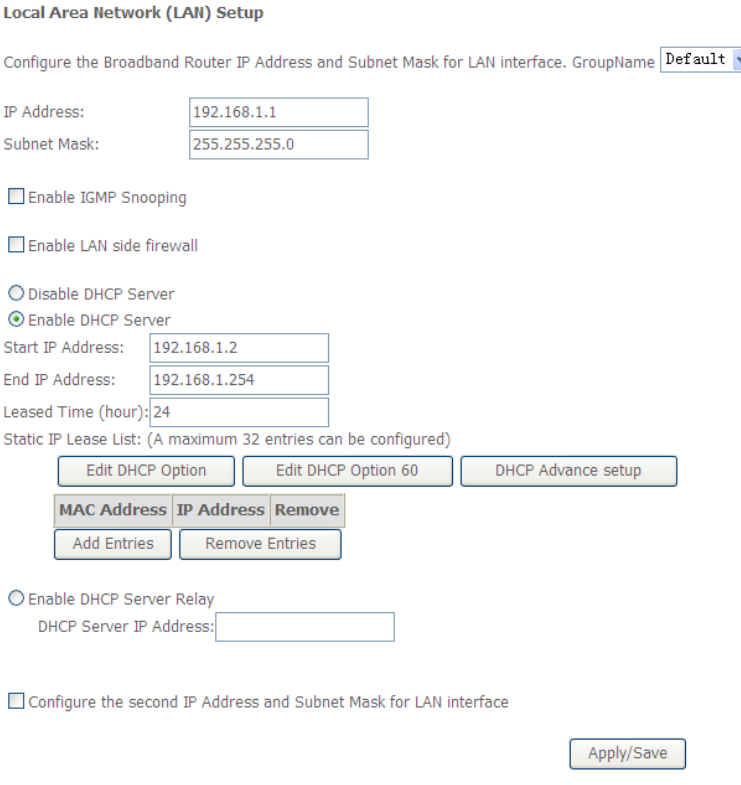
Figure 39 Bridge summary

Step4 In this page, it displays the information about the bridge settngs. Click **Apply/Save** to save and apply the settings. You can modify the settings by clicking the **Back** button if necessary.

5.3.3 LAN Configuration

5.3.3.1 IPv4 Autoconfig

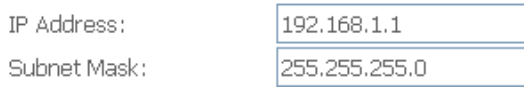
Choose **Advanced Setup > LAN > IPv4 Autoconfig**, and the following page appears.



In this page, you can configure an IP address for the DSL router, enable IGMP snooping, enable or disable the DHCP server, edit the DHCP option, configure the

DHCP advanced setup and set the binding between a MAC address and an IP
address.

Configuring a Private IP Address for the DSL Router



In this page, you can modify the IP address of the device. The preset IP address is 192.168.1.1.

Enabling IGMP Snooping

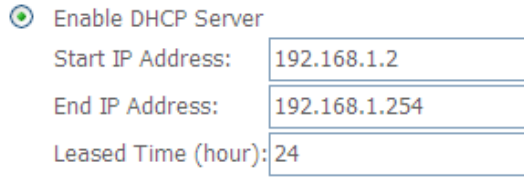
IGMP snooping enables the router to forward multicast traffic intelligently, instead of flooding all ports in the VLAN. With IGMP snooping, the router listens to IGMP membership reports, queries and leave messages to identify the switch ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group or groups.

Enabling the LAN Side Firewall

Firewall can prevent unexpected traffic on the Internet from your host in the LAN.

In this page, you can enable or disable the LAN side firewall.

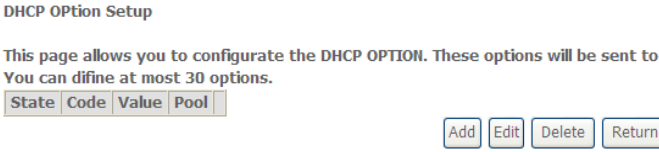
Configuring the DHCP Server



If you enable the DHCP sever, the clients will automatically acquire the IP address from the DHCP server. If the DHCP server is disabled, you need to manually set the start IP address, end IP address and lease time for clients in the LAN.

Editing the DHCP Option

Click the **Edit DHCP Option** button in the **Local Area Network (LAN) Setup** page to display the **DHCP Option Setup** page.



In this page, you can add, edit or delete the DHCP options, and these options will be sent to the DHCP client.

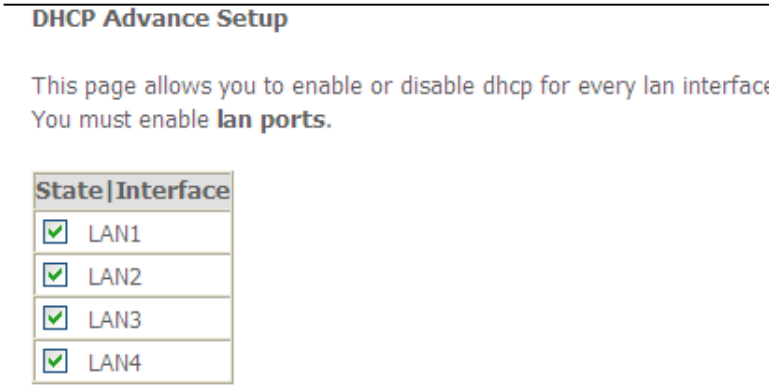
Editing the DHCP Option60

Click the **Edit DHCP Option60** button in the **Local Area Network (LAN) Setup** page to display the **DHCP Option60 Setup** page.

In this page, you can add, edit or delete the DHCP60 options.

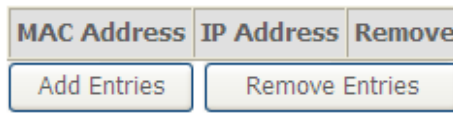
DHCP Advanced Setup

Click the **DHCP Advance Setup** button in the **Local Area Network (LAN) Setup** page to display the following page. In this page, you can enable or disable DHCP for every LAN interface.



Configuring the DHCP Static IP Lease List

The lease list of static IP address reserves static IP addresses for the hosts with specific MAC addresses. When a host whose MAC address is in the lease list of static IP address requests the DHCP server for an IP address, the DHCP server assigns the reserved IP address to the host.

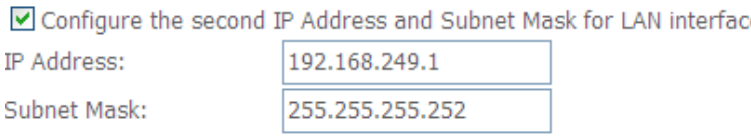


Click the **Add Entries** button in the **Local Area Network (LAN) Setup** page to display the **DHCP Static IP Lease** page.

In this page, enter the MAC address of the LAN host and the static IP address reserved for the host, and then click the **Apply/Save** button to apply the settings.

Configuring the Second IP Address and Subnet Mask for a LAN Interface

In the **Local Area Network (LAN) Setup** page, you may set the second IP address and the subnet mask for a LAN interface.

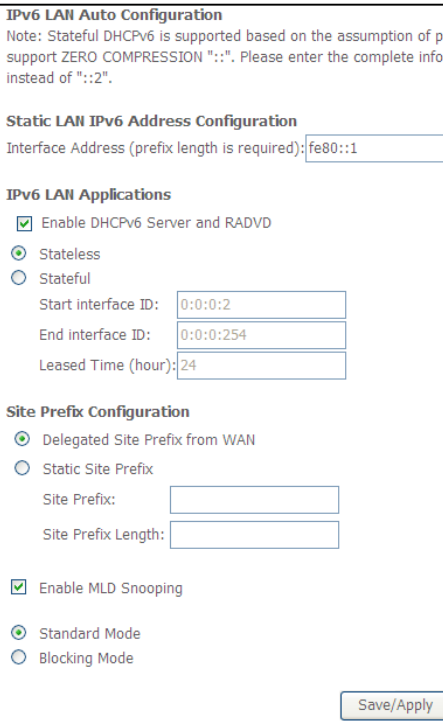


After enabling **Configure the second IP Address and Subnet Mask for LAN interface**, enter an IP address and a subnet mask for the LAN interface.

After finishing setting, click the **Apply/Save** button to apply the settings.

5.3.3.2 IPv6 Autoconfig

Choose **Advanced Setup > LAN > IPv6 Autoconfig**, and the following page appears.


IPv6 LAN Auto Configuration
Note: Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information. For exampe, Please enter "0:0:0:2" instead of "::2".
Static LAN IPv6 Address Configuration
Interface Address (prefix length is required): fe80::1
IPv6 LAN Applications
Enable DHCPv6 Server and RADVD
Stateless
Stateful
Start interface ID: 0:0:0:2
End interface ID: 0:0:0:254
Leased Time (hour): 24
Site Prefix Configuration
Delegated Site Prefix from WAN
Static Site Prefix
Site Prefix:
Site Prefix Length:
Enable MLD Snooping
Standard Mode
Blocking Mode
Save/Apply

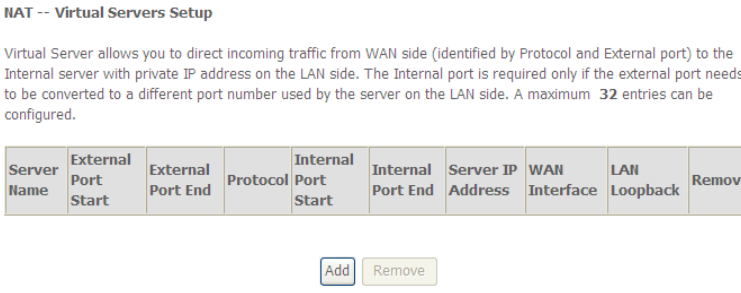
In this page, you can configure a static LAN IPv6 address, enable or disable DHCPv6 server and RADVD, configure site prefix, and enable or disable MLD
Snooping.
After finishing setting, click the **Apply/Save** button to apply the settings.

5.3.4 NAT

5.3.4.1 Virtual Servers

Firewall can prevent unexpected traffic on the Internet from your host on the LAN. The virtual server can create a channel that can pass through the firewall. In that case, the host on the Internet can communicate with a host on your LAN within certain port range.

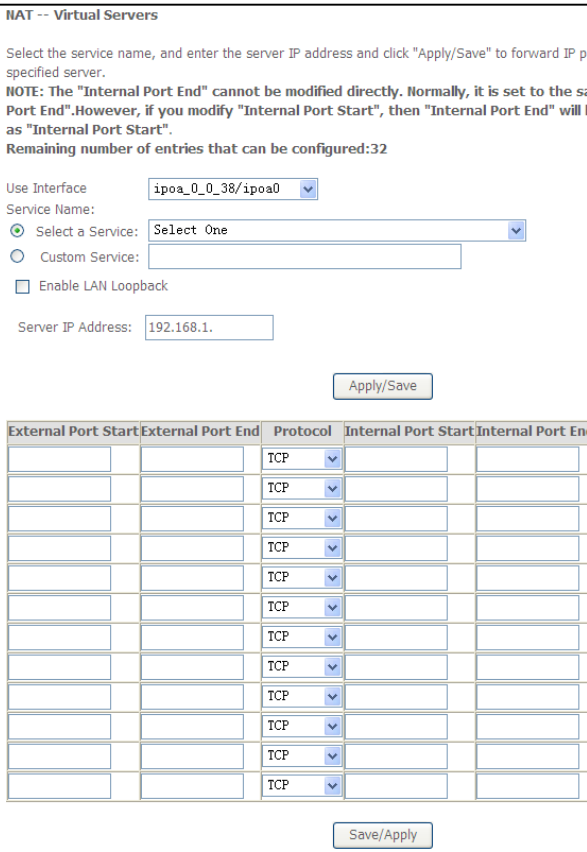
Choose **Advanced Setup > NAT > Virtual Servers**, and the following page appears.


NAT -- Virtual Servers Setup
Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.
Server Name
External Port Start
External Port End
Protocol
Internal Port Start
Internal Port End
Server IP Address
WAN Interface
LAN Loopback
Remove
Add
Remove

In this page, you are allowed to add or remove a virtual server entry.

To add a virtual server, do as follows:

Step 1 Click the **Add** button to display the following page.


NAT -- Virtual Servers
Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server.
NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End".However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".
Remaining number of entries that can be configured:32
Use Interface
ipoa_0_0_38/ipoa0
Service Name:
Select a Service:
Select One
Custom Service:
Enable LAN Loopback
Server IP Address:
192.168.1.
Apply/Save
External Port Start
External Port End
Protocol
Internal Port Start
Internal Port End
TCP
Save/Apply

- **Use interface**: Select an interface that you want to configure.
- **Select a Service**: Select a proper service in the drop-down list.
- **Custom Server**: Enter a new service name to establish a user service type.
- **Server IP Address**: Assign an IP address to virtual server.
- **External Port Start**: When selecting a service, the port number will automatically be displayed. You can modify it if necessary.
- **External Port End**: When selecting a service, the port number will automatically be displayed. You can modify it if necessary.

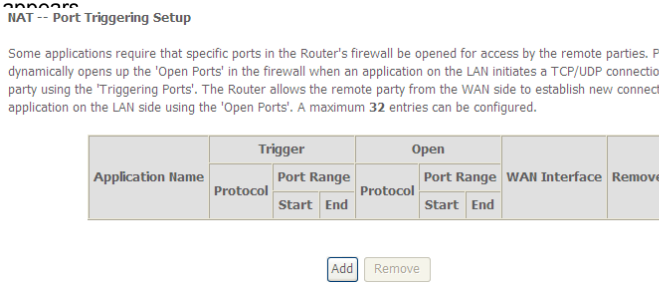
- **Protocol**: You may select TCP/UDP, TCP, or UDP in the drop-down list.
- **Internal Port Start**: When selecting a service, the port number will automatically be displayed. You can modify it if necessary.
- **Internal Port End**: When selecting a service, the port number will automatically be displayed. You can modify it if necessary.

Step 2 After finishing setting, click **Save/Apply** to save and apply the settings.

5.3.4.2 Port Triggering

Some applications need some ports to be opened in the firewall for the remote access. When an application initializes a TCP/UDP to connect to a remote user, port triggering dynamically opens the open ports of the firewall.

Choose **Advanced Settings > NAT > Port Triggering**, and the following page appears.


NAT -- Port Triggering Setup

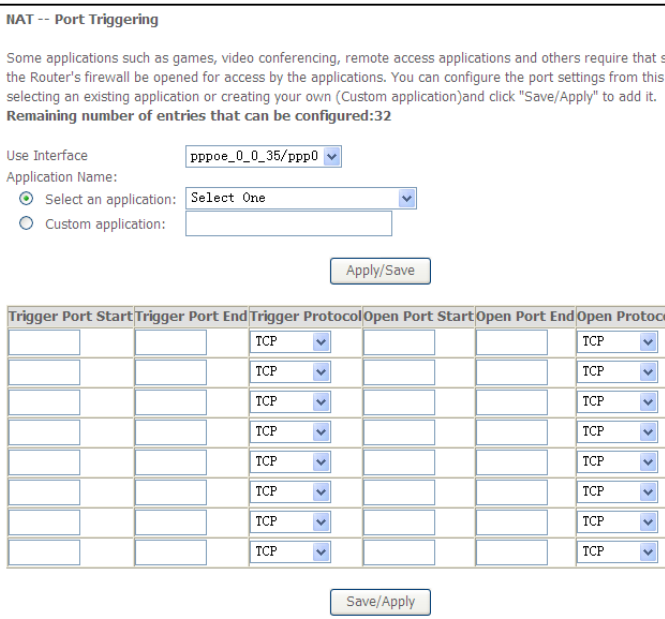
Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Application Name	Trigger			Open			WAN Interface	Remove
	Protocol	Port Range		Protocol	Port Range			
		Start	End		Start	End		

Add Remove

In this page, you may add or remove an entry of port triggering.

Click the **Add** button to display the following page.


NAT -- Port Triggering
Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application)and click "Save/Apply" to add it.
Remaining number of entries that can be configured:32
Use Interface
pppoe_0_0_35/ppp0
Application Name:
Select an application:
Select One
Custom application:
Apply/Save
Trigger Port Start
Trigger Port End
Trigger Protocol
Open Port Start
Open Port End
Open Protocol
TCP
Save/Apply

- **Use interface**: Select an interface that you want to configure.
- **Select an application:** Select a proper application in the drop-down list.
- **Custom application:** Manually define an application.
- **Trigger port Start:** The start port number that LAN uses to trigger the open port.
- **Trigger port End:** The end port number that LAN uses to trigger the open port.
- **Trigger Protocol:** Select the application protocol. You may select TCP/UDP, TCP, or UDP.
- **Open Port Start:** The start port number that is opened to WAN.
- **Open Port End:** The end port number that is opened to WAN.
- **Open Protocol:** Select the proper protocol that is opened to WAN. You may select TCP/UDP, TCP, or UDP.

After finishing setting, click **Save/Apply** to apply the settings.

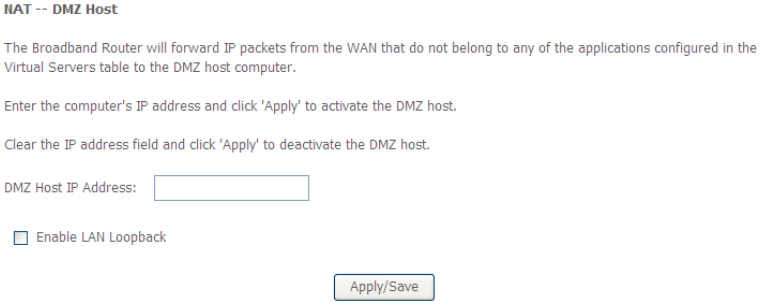
✍ **Note:**

You can use a single port number, several port numbers separated by commas,
port blocks consisting of two port numbers separated by a dash, or any combination of these, for example 80, 90-140, 180.

5.3.4.3 DMZ Host

DMZ allows all the ports of a PC on your LAN to be exposed to the Internet. Set the IP address of the PC to be DMZ host, so that the DMZ host will not be blocked by firewall.

Choose **Advanced Setup > NAT > DMZ host** to display the following page.

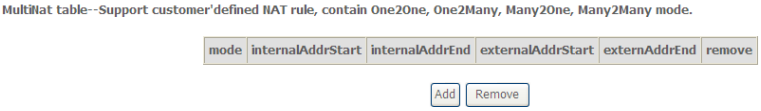

NAT -- DMZ Host
The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.
Enter the computer's IP address and click 'Apply' to activate the DMZ host.
Clear the IP address field and click 'Apply' to deactivate the DMZ host.
DMZ Host IP Address:
Enable LAN Loopback
Apply/Save

In this page, enter the IP address of the DMZ host. You may also enable LAN
Loopback.
After finishing the settings, click the **Apply/Save** button to apply the settings.

To clear the DMZ function of the host, delete the IP address of the host in the field of **DMZ Host IP Address**, and then click the **Apply/Save** button.

5.3.4.4 Multi Nat

Choose **Advanced Setup > NAT > Multi Nat** to display the following page.



Multi-NAT can be used where you have multiple public IP addresses allocated by your ISP. Instead of a many-to-one relationship, you can have a one-to-one relationship between a public IP address and an internal/private IP address. This means that you have the protection of NAT (see earlier) but the PC can be addressed directly from the outside world by its aliased public IP address through opening specific ports to it (for example TCP port 80 for an http/web server).

5.3.5 Security

By default, the firewall is enabled. The firewall is used to block the file transmission between the Internet and your PC. It serves as a safety guard and permits only the authorized files to be sent to the LAN.

✍ **Note:**

If the DSL router is configured as bridge mode, IP filtering is disabled.

Outgoing IP Filtering Setup

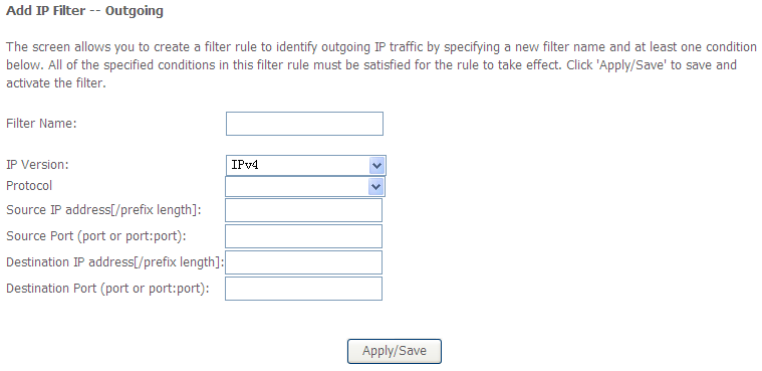
When the outgoing IP filtering settings is enabled on the DSL router, the security functions for the local network are enabled at the same time.

Choose **Security > IP Filtering >Outgoing** and the following page appears.

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be blocked by setting filters.

In this page, you may add or remove the outgoing IP filtering rules.

Click the **Add** button to display the following page.


Add IP Filter -- Outgoing
The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.
Filter Name:
IP Version:
IPv4
Protocol
Source IP address[/prefix length]:
Source Port (port or port:port):
Destination IP address[/prefix length]:
Destination Port (port or port:port):
Apply/Save

In this page, you can create a filter rule to identify the outgoing IP traffic by specifying a new filter name and at least one condition.

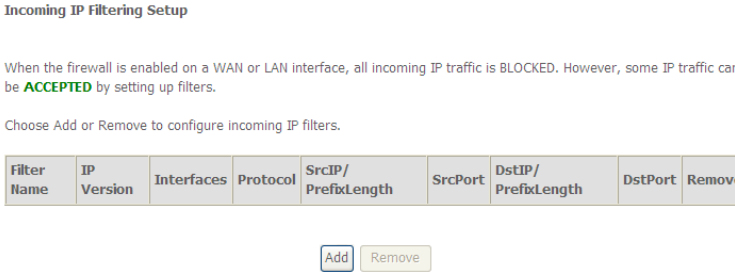
- **Filter Name:** Set the filter name.
- **IP Version:** Select the proper IP version in the drop-down list.
- **Protocol:** Select a protocol that needs to be filtered.
- **Source IP address [/prefix length]**: Set the range of local IP address.
- **Source Port (port or port: port)**: Set the local port.
- **Destination IP address [/prefix length]**: Set the range of IP address of the exterior network.
- **Destination Port (port or port: port)**: Set the port of the exterior network.

After finishing setting, click **Apply/Save** to save and activate the filtering rule.

Incoming IP Filtering Setup

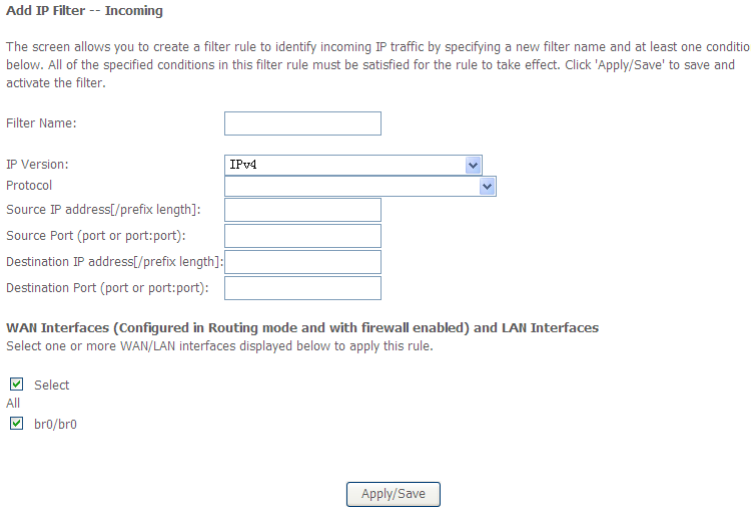
The incoming IP filter is used to block and permit the IP packet transmisstion from the internet.

Choose **Security > IP Filtering >Incoming** and the following page appears.


Incoming IP Filtering Setup
When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be ACCEPTED by setting up filters.
Choose Add or Remove to configure incoming IP filters.
Filter Name
IP Version
Interfaces
Protocol
SrcIP/ PrefixLength
SrcPort
DstIP/ PrefixLength
DstPort
Remove
Add
Remove

In this page, you can add or remove the incoming IP filtering rules.

Click the **Add** button to display the following page.


Add IP Filter -- Incoming
The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.
Filter Name:
IP Version:
IPv4
Protocol
Source IP address[/prefix length]:
Source Port (port or port:port):
Destination IP address[/prefix length]:
Destination Port (port or port:port):
WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces
Select one or more WAN/LAN interfaces displayed below to apply this rule.
Select All
br0/br0
Apply/Save

In this page, you can create a filter rule to identify the incoming IP traffic by specifying a new filter name and at least one condition, and you must select at least one WAN interface for the rule.

- **Filter Name:** Set the filter name.
- **IP Version:** Select the proper IP version in the drop-down list.
- **Protocol:** Select a protocol that needs to be filtered.
- **Source IP address [/prefix length]**: Set the range of local IP address.

- **Source Port (port or port: port)**: Set the local port.
- **Destination IP address [/prefix length]**: Set the range of IP address of the exterior network.
- **Destination Port (port or port: port)**: Set the port of the exterior network.

After finishing setting, click **Apply/Save** to save and activate the filtering rule.

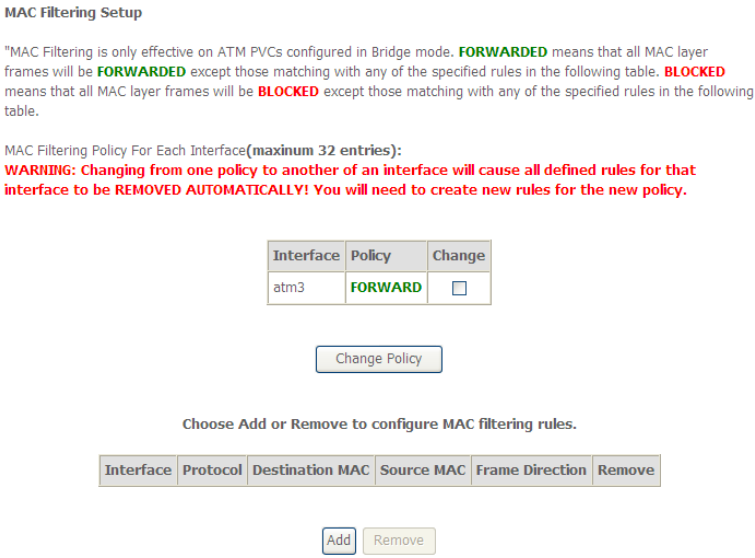
MAC Filtering Setup

In some cases, you may want to manage Layer2 MAC address to block or permit a computer within the home network. When you enable MAC filter rules, the DSL router serves as a firewall that works at layer 2.

Note:

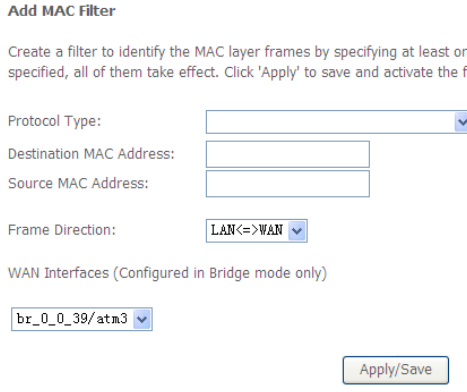
MAC filtering is only effective on ATM PVCs configured in bridge mode.

Choose **Security** > **MAC Filtering** and the following page appears.


MAC Filtering Setup
"MAC Filtering is only effective on ATM PVCs configured in Bridge mode. FORWARDED means that all MAC layer frames will be FORWARDED except those matching with any of the specified rules in the following table. BLOCKED means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table.
MAC Filtering Policy For Each Interface(maxinum 32 entries):
WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.
Interface
Policy
Change
atm3
FORWARD
Change Policy
Choose Add or Remove to configure MAC filtering rules.
Interface
Protocol
Destination MAC
Source MAC
Frame Direction
Remove
Add
Remove

In this page, you can add or remove the MAC filtering rule. You may change the MAC filtering policy from **FORWARDED** to **BLOCKED** by clicking the **Change Policy** button.

Click the **Add** button to display the following page.


Add MAC Filter
Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click 'Apply' to save and activate the filter.
Protocol Type:
Destination MAC Address:
Source MAC Address:
Frame Direction:
LAN<=>WAN
WAN Interfaces (Configured in Bridge mode only)
br_0_0_39/atm3
Apply/Save

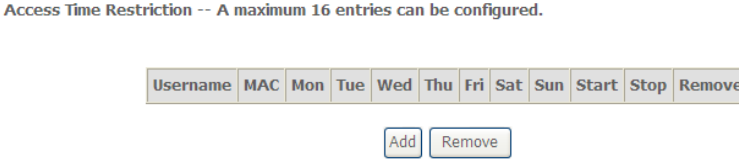
- **Protocol Type**: Select the proper protocol type.
- **Destination MAC Address**: Enter the destination MAC address.
- **Source MAC Address**: Enter the source MAC address.
- **Frame Direction**: The direction of transmission frame.
- **WAN Interface (Configured in bridge mode only)**: Select the proper WAN interface in the drop-down list.

After finishing setting, click **Apply/Save** to save and apply the filtering rule.

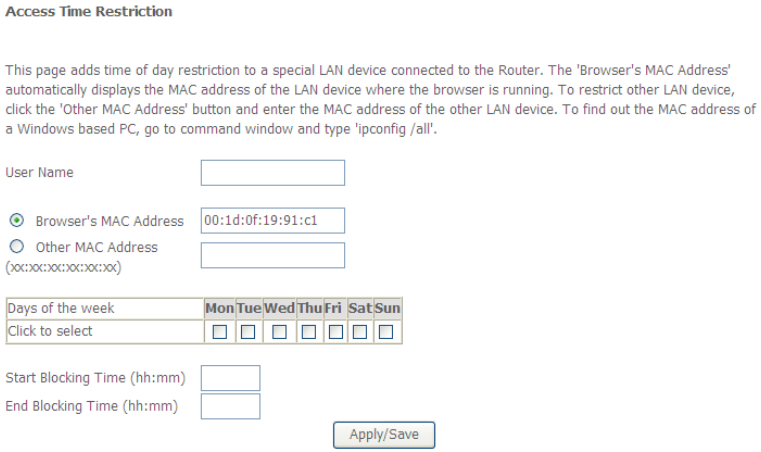
5.3.6 Parental Control

Time Restriction

Choose **Advanced Setup** > **Parental Control** > **Time Restriction**, and the following page appears.



Click the **Add** button to display the following page.

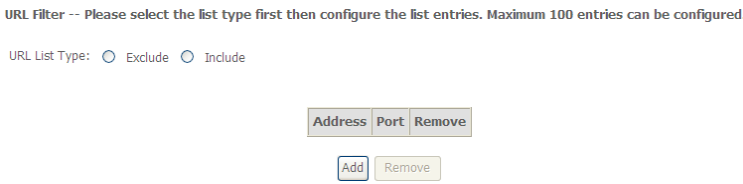

Access Time Restriction
This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the 'Other MAC Address' button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type 'ipconfig /all'.
User Name
Browser's MAC Address
00:1d:0f:19:91:c1
Other MAC Address
(xx:xx:xx:xx:xx:xx)
Days of the week
Mon Tue Wed Thu Fri Sat Sun
Click to select
Start Blocking Time (hh:mm)
End Blocking Time (hh:mm)
Apply/Save

This page is used to control the time restriction to a special LAN device that connects to the DSL router. In this page, enter the user name and configure the time settings.

After finishing setting, click the **Apply/Save** button to save and apply the settings.

Url Filter

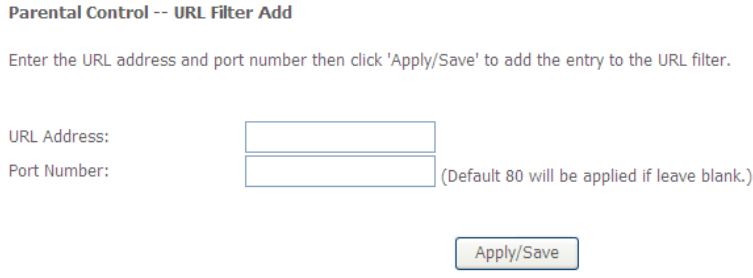
Click **Advanced Setup** > **Parental Contro**l > **Url Filter**, and the following page appears.


URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.
URL List Type: Exclude Include
Address Port Remove
Add Remove

Thisp age is used to prevent the LAN users from accessing some Websites in the WAN.

In this page, you may select the **Exclude** URL list type or the **Include** URL list type. If you select the **Exclude** URL list type, it means that the URLs in the list are not accessible. If you select the select the **Include** URL list type, you are allowed to access the the URLs in the list.

Click the **Add** button to display the following page.

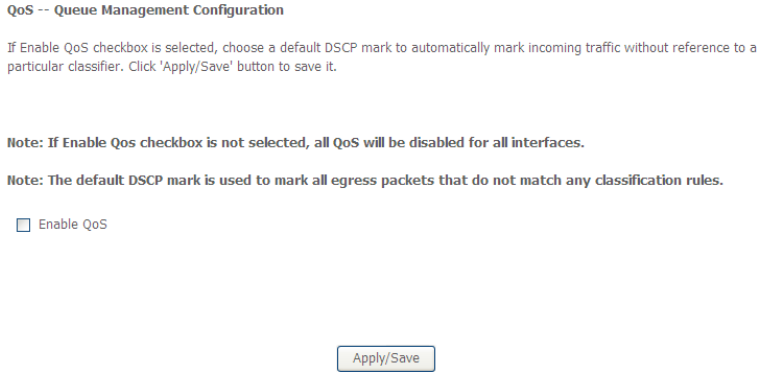

Parental Control -- URL Filter Add
Enter the URL address and port number then click 'Apply/Save' to add the entry to the URL filter.
URL Address:
Port Number:
(Default 80 will be applied if leave blank.)
Apply/Save

In this page, enter the URL address and its corresponding port number. For example, enter the URL address ***http://www.google.com*** and the port number **80**, and then click the **Apply/Save** button. See the following figure:

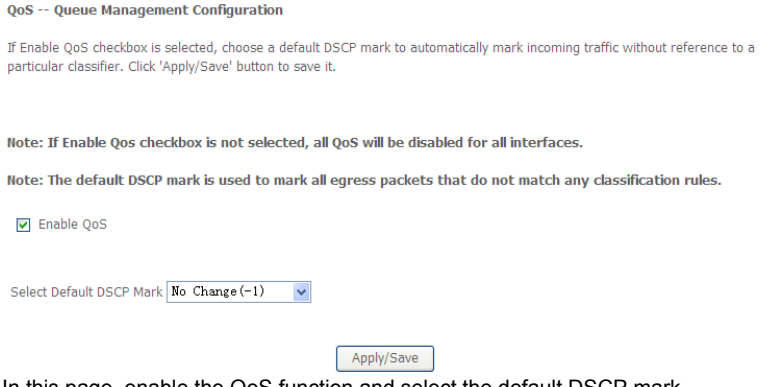
5.3.7 Quality of Service

Enabling QoS

Choose **Advance Setup > Quality of Service** and the following page appears.


QoS -- Queue Management Configuration
If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.
Note: If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.
Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.
Enable QoS
Apply/Save

Select **Enable QoS** to enable QoS and configure the default DSCP mark.


QoS -- Queue Management Configuration
If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.
Note: If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.
Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.
Enable QoS
Select Default DSCP Mark
No Change(-1)
Apply/Save

In this page, enable the QoS function and select the default DSCP mark.

After finishing setting, click **Apply/Save** to save and apply the settings.

✍ **Note:**

If the **Enable Qos** checkbox is not selected, all QoS will be disabled for all interfaces. The default DSCP mark is used to mark all egress packets that do not match any classification rules.

Queue Configuration

Choose **Advanced Setup** > **Quality of Service** > **Queue Config**, and the following page appears.

QoS Queue Setup

In ATM mode, maximum 16 queues can be configured.
In PTM mode, maximum 8 queues can be configured.
For each Ethernet interface, maximum 4 queues can be configured.
If you disable WMM function in Wireless Page, queues related to wireless will not take effects

The QoS function has been disabled. Queues would not take effects.

Name	Key	Interface	Scheduler	Precedence	Weight	DSL Latency	PTM Priority	Enable	Remove
WMM Voice Priority	1	wl0	SP	1				Enabled	
WMM Voice Priority	2	wl0	SP	2				Enabled	
WMM Video Priority	3	wl0	SP	3				Enabled	
WMM Video Priority	4	wl0	SP	4				Enabled	
WMM Best Effort	5	wl0	SP	5				Enabled	
WMM Background	6	wl0	SP	6				Enabled	
WMM Background	7	wl0	SP	7				Enabled	
WMM Best Effort	8	wl0	SP	8				Enabled	
Default Queue	33	atm0	SP	8		Path0		☐	
Default Queue	34	atm1	SP	8		Path0		☐	
Default Queue	35	atm2	SP	8		Path0		☐	
Default Queue	36	ipoa0	SP	8		Path0		☐	

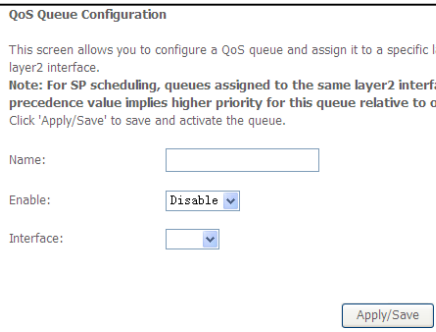
Add Enable Remove

In this page, you can enable, add or remove a QoS rule.

✍ **Note:**

The lower integer value for precedence indicates the higher priority.

Click the **Add** button to display the following page.

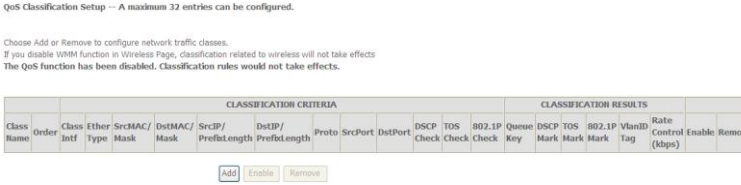

QoS Queue Configuration
This screen allows you to configure a QoS queue and assign it to a specific layer2 interface. The scheduler algorithm is defined by the layer2 interface.
Note: For SP scheduling, queues assigned to the same layer2 interface shall have unique precedence. Lower precedence value implies higher priority for this queue relative to others
Click 'Apply/Save' to save and activate the queue.
Name:
Enable:
Disable
Interface:
Apply/Save

- **Name:** Enter the name of QoS queue.
- **Enable:** Enable or disable the QoS queue.
- **Interface:** Select the proper interface for the QoS queue.

After finishing setting, click **Apply/Save** to save and apply the settings.

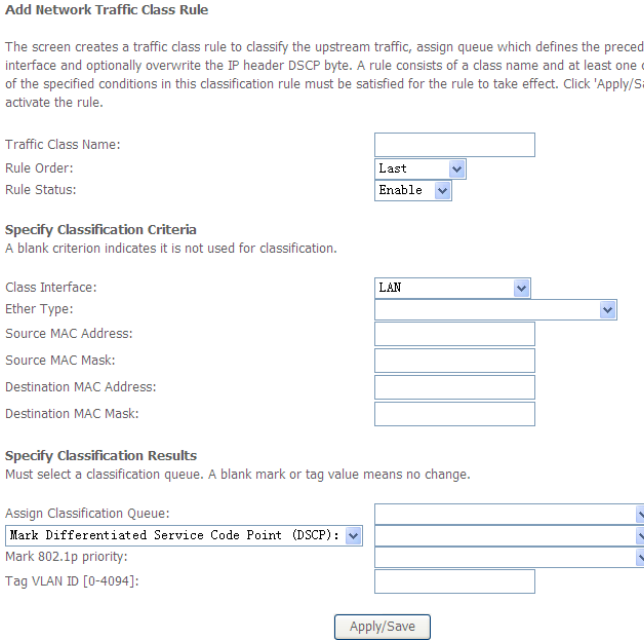
QoS Classification

Choose **Advanced Setup** > **Quality of Service** > **Qos Classification** and the following page appears.



In this page, you can enable, add or remove a QoS classification rule.

Click the **Add** button to display the following page.


Add Network Traffic Class Rule
The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the rule.
Traffic Class Name:
Rule Order:
Last
Rule Status:
Enable
Specify Classification Criteria
A blank criterion indicates it is not used for classification.
Class Interface:
LAN
Ether Type:
Source MAC Address:
Source MAC Mask:
Destination MAC Address:
Destination MAC Mask:
Specify Classification Results
Must select a classification queue. A blank mark or tag value means no change.
Assign Classification Queue:
Mark Differentiated Service Code Point (DSCP):
Mark 802.1p priority:
Tag VLAN ID [0-4094]:
Apply/Save

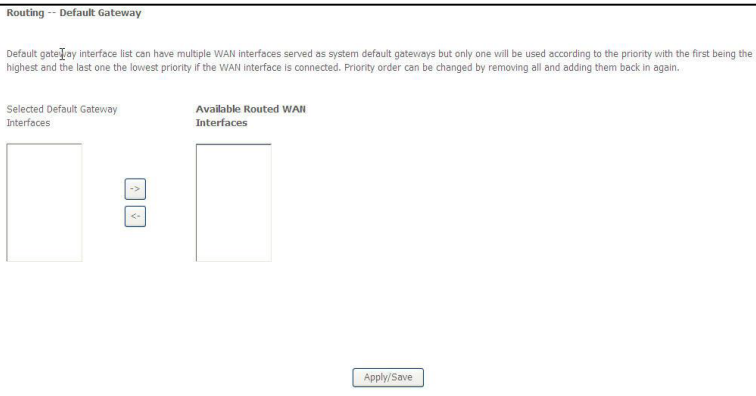
In this page, enter the traffic name, select the rule order and the rule status, and specify the classification criteria and the classification results.

After finishing setting, click **Apply/Save** to save and apply the settings.

5.3.8 Routing

Default Gateway

Choose **Advanced Setup** > **Routing** > **Default Gateway**, and the following page appears.


Routing -- Default Gateway
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Selected Default Gateway Interfaces
Available Routed WAN Interfaces
->
<-
Apply/Save

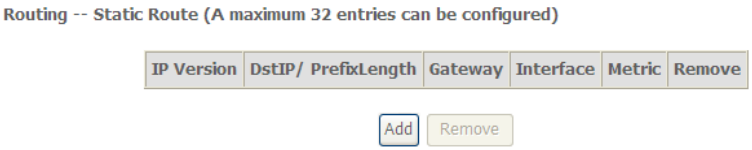
In this page, you can modify the default gateway settings.

Select a proper WAN interface and add it to the column of **Selected Default Gateway Interfaces** as the system default gateway.

After finishing setting, click **Apply/Save** to save and apply the settings.

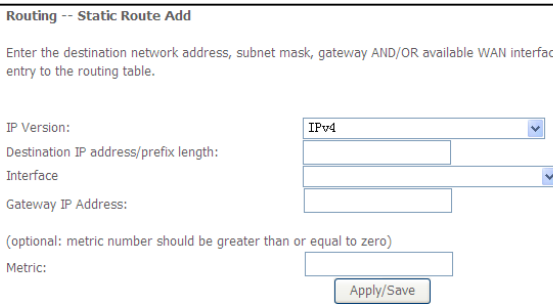
Static Route

Choose **Advanced Setup** > **Routing** > **Static Route** and the following page appears.



In this page, you can add or remove a static routing rule.

Click the **Add** button to display the following page.

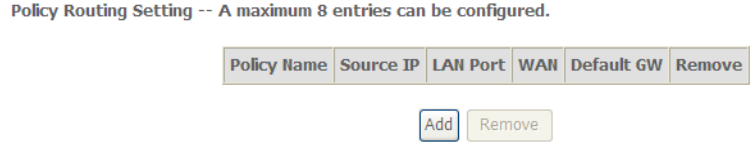

Routing -- Static Route Add
Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click 'Apply/Save' to add the entry to the routing table.
IP Version:
IPv4
Destination IP address/prefix length:
Interface
Gateway IP Address:
(optional: metric number should be greater than or equal to zero)
Metric:
Apply/Save

- **IP Version:** Select the IP version to be IPv4.
- **Destination IP address/prefix length:** Enter the destination IP address.
- **Interface:** select the proper interface for the rule.
- **Gateway IP Address:** The next-hop IP address.
- **Metric:** The metric value of routing.

After finishing setting, click **Apply/Save** to save and apply the settings.

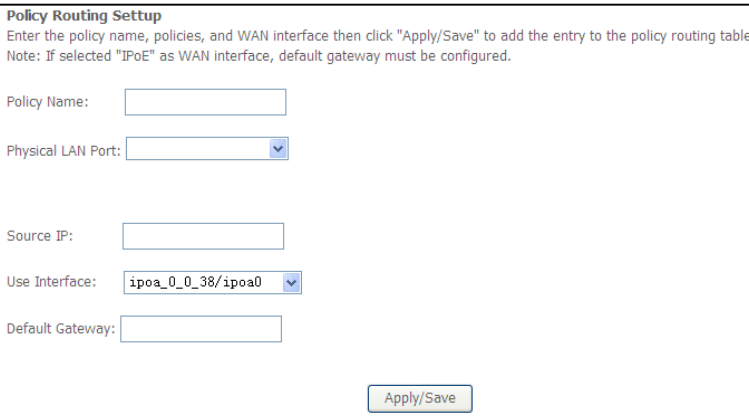
Policy Routing

Choose **Advanced Setup** > **Routing** > **Policy Routing** and the following page appears.



In this page, you can add or remove a static policy rule.

Click the **Add** button to display the following page.

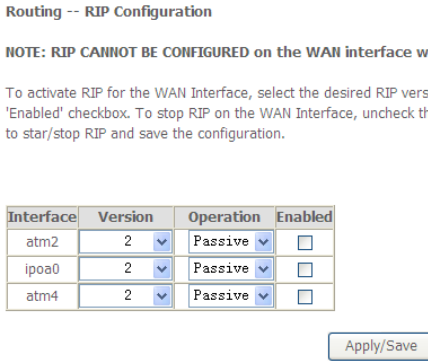

Policy Routing Settup
Enter the policy name, policies, and WAN interface then click "Apply/Save" to add the entry to the policy routing table.
Note: If selected "IPoE" as WAN interface, default gateway must be configured.
Policy Name:
Physical LAN Port:
Source IP:
Use Interface:
ipoa_0_0_38/ipoa0
Default Gateway:
Apply/Save

In this page, enter the policy name, source IP and default gateway, and select the physical LAN port and interface.

After finishing setting, click **Apply/Save** to save and apply the settings.

RIP

Choose **Advanced Setup > Routing > RIP** and the following page appears.

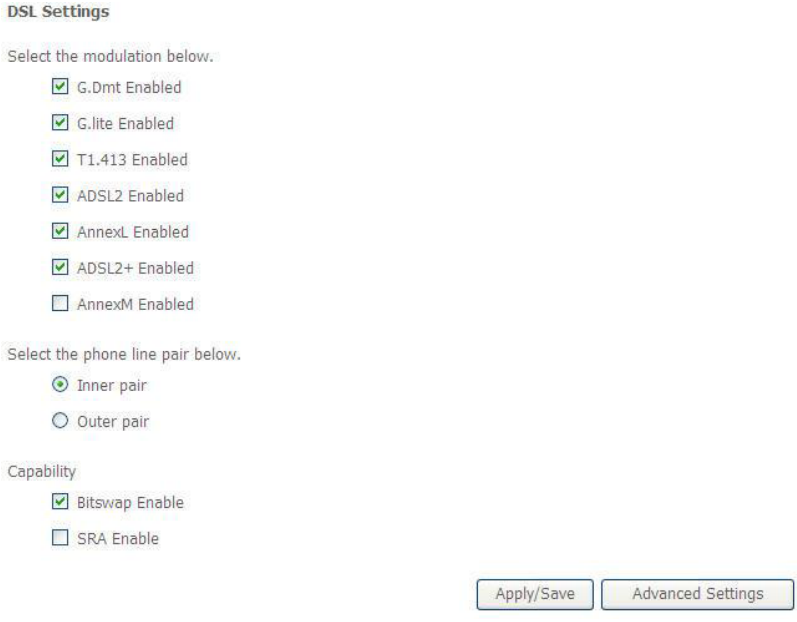

Routing -- RIP Configuration
NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).
To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.
Interface
Version
Operation
Enabled
atm2
2
Passive
ipoa0
2
Passive
atm4
2
Passive
Apply/Save

In this page, to configure an individual interface, select the desired RIP version and operation, and then select the **Enabled** checkbox for the interface.

After finishing setting, click **Apply/Save** to save and apply the settings.

5.3.9 DSL

Choose **Advanced Setup** > **DSL** and the following page appears. In this page, you can view the DSL settings. Usually, you can keep this factory default setting. The modem negotiates the modulation mode with the DSLAM.

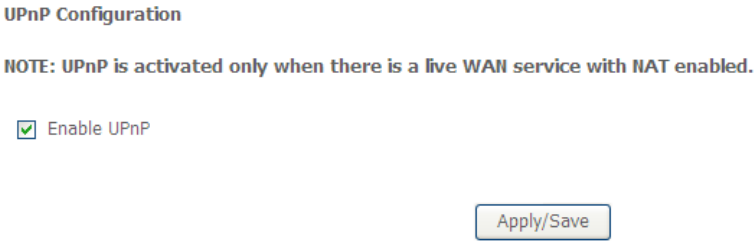


In this page, you can set the DSL settings. Usually, you do not need to modify the factory default settings.

After finishing setting, click **Apply/Save** to save and apply the settings.

5.3.10 UPnP

Choose **Advanced Setup > UPnP** and the following page appears.

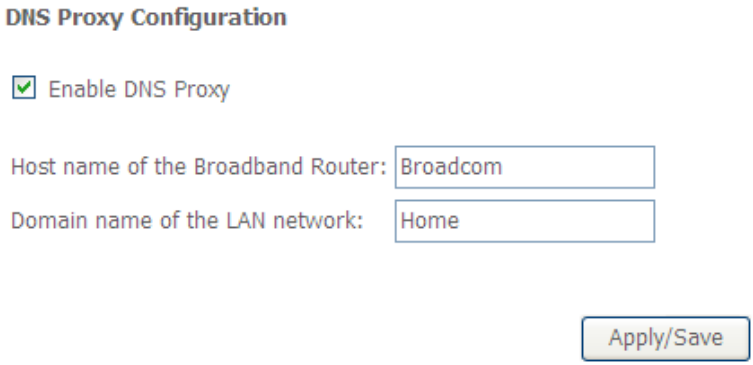


In this page, you can enable or disable the UPnP function.

After finishing setting, click **Apply/Save** to save and apply the settings.

5.3.11 DNS Proxy

Choose **Advanced Setup > DNS Proxy** and the following page appears.



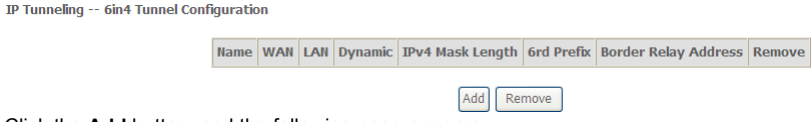
In this page, you can enable or disable the DNS proxy function.

After enabling the DNS proxy function, enter the host name of the broadband router and the domain name of the LAN network, and then click **Apply/Save** to save and apply the settings.

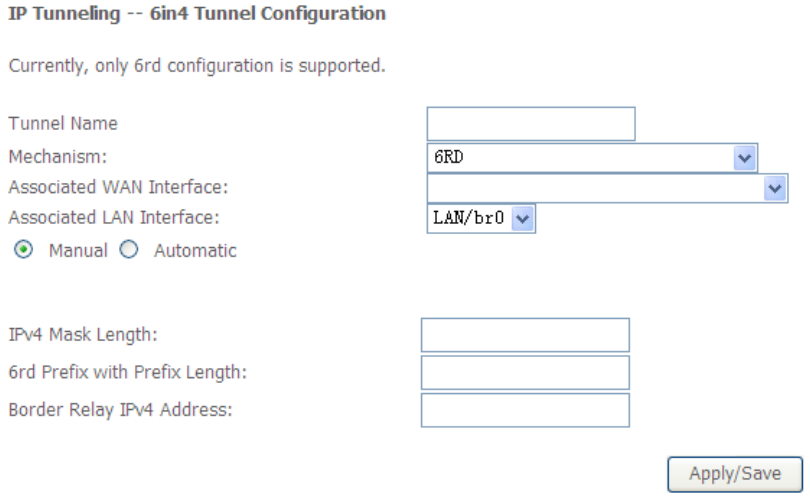
5.3.12 IP Tunnel

IPv6inIPv4

Choose **Advanced Setup > IP Tunnel > IPv6inIPv4**, and the following page appears.



Click the **Add** button, and the following page appears.

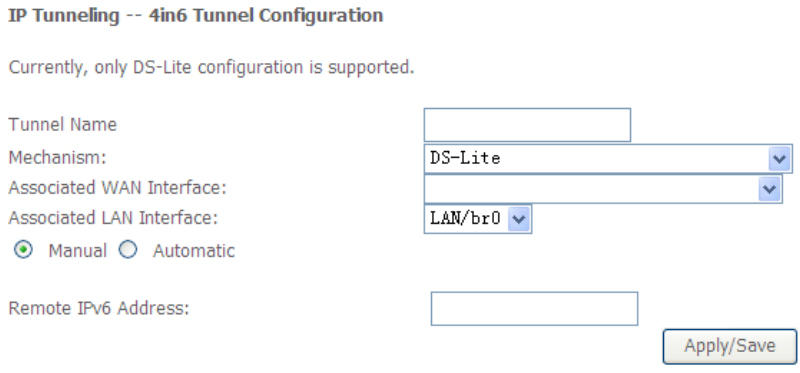


Click **Apply/Save** to save and enable the settings.

IPv4inIPv6

Choose **Advanced Setup > IP Tunnel > IPv4inIPv6**, and the following page appears.

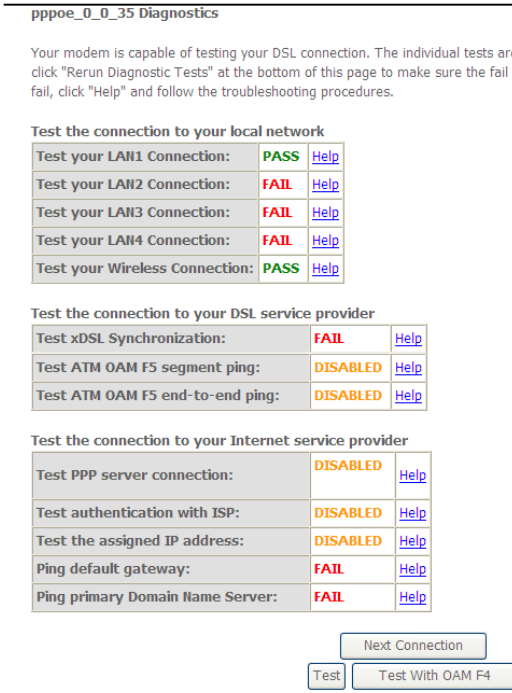
Click the **Add** button, and the following page appears.



Click **Apply/Save** to save and enable the settings.

5.4 Diagnostics

Click **Diagnostics** > **Diagnostics**, and the following page appears.


pppoe_0_0_35 Diagnostics

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your LAN1 Connection:	PASS	Help
Test your LAN2 Connection:	FAIL	Help
Test your LAN3 Connection:	FAIL	Help
Test your LAN4 Connection:	FAIL	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your DSL service provider

Test xDSL Synchronization:	FAIL	Help
Test ATM OAM F5 segment ping:	DISABLED	Help
Test ATM OAM F5 end-to-end ping:	DISABLED	Help

Test the connection to your Internet service provider

Test PPP server connection:	DISABLED	Help
Test authentication with ISP:	DISABLED	Help
Test the assigned IP address:	DISABLED	Help
Ping default gateway:	FAIL	Help
Ping primary Domain Name Server:	FAIL	Help

Next Connection

Test | Test With OAM F4

Your modem is capable of testing your DSL connection. The individual tests are listed. If a test displays a fail status, click **Test** at the bottom of this page to make sure the fail status is consistent. If test failure continues, click **Help** and follow the troubleshooting procedures.

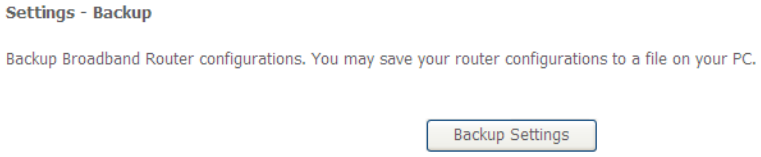
5.5 Management

Choose **Management** and the submenus include **Settings**, **System Log**, **TR-069 Client**, **Access Control**, **Update Software** and **Reboot**.

5.5.1 Settings

Backup

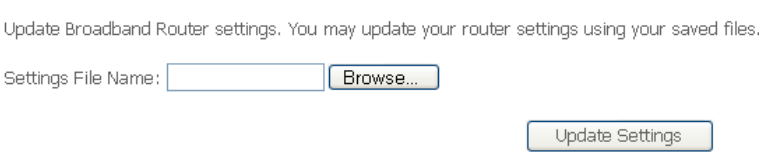
Choose **Management > Settings > Backup** to display the following page.


Settings - Backup
Backup Broadband Router configurations. You may save your router configurations to a file on your PC.
Backup Settings

In this page, click the **Backup Settings** button to save your router's settings to your local PC.

Update

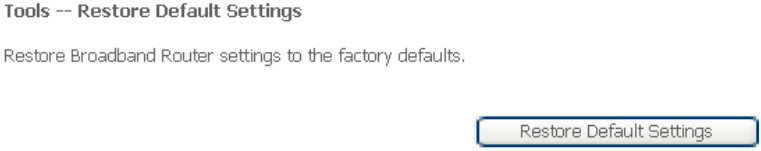
Choose **Management > Settings > Update**, and the following page appears.


Tools -- Update Settings
Update Broadband Router settings. You may update your router settings using your saved files.
Settings File Name:
Browse...
Update Settings

In this page, click the **Browse…** button to select the correct new settings file, and then click the **Update Settings** button to update the router's settings.

Restore Default

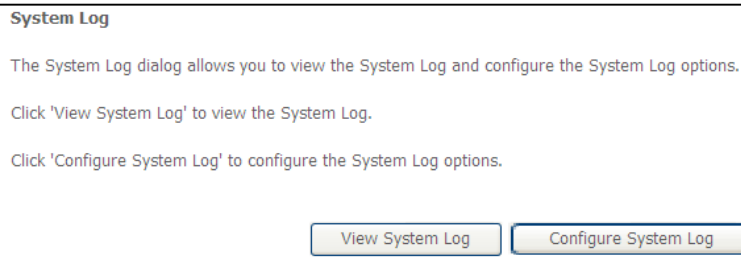
Choose **Management > Settings > Restore Default** to display the following page.



In this page, click the **Restore default settings** button, and then system returns to the default settings.

5.5.2 System Log

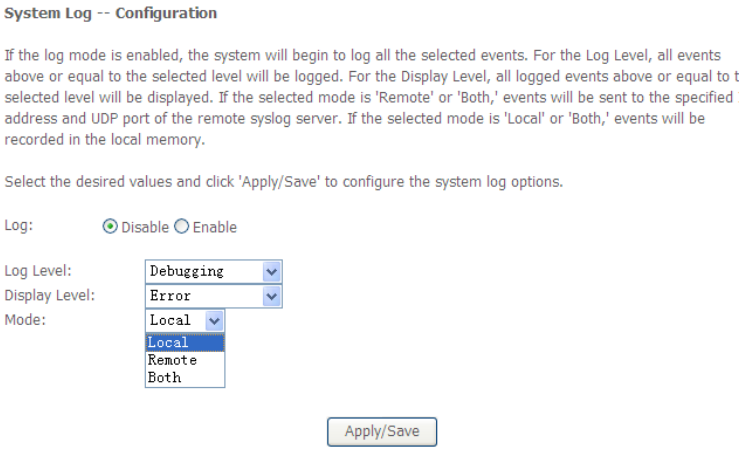
Choose **Management > System Log** to display the following page.


System Log
The System Log dialog allows you to view the System Log and configure the System Log options.
Click 'View System Log' to view the System Log.
Click 'Configure System Log' to configure the System Log options.
View System Log
Configure System Log

In this page, you can configure and view the system log.

Configuring System Log

Click the **Configure System Log** button to display the following page.


System Log -- Configuration
If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.
Select the desired values and click 'Apply/Save' to configure the system log options.
Log: Disable Enable
Log Level: Debugging
Display Level: Error
Mode: Local
Local
Remote
Both
Apply/Save

In this page, you can set 3 types of system log modes: **Local**, **Remote** and **Both**.

- **Local:** When selecting **Local**, the events are recorded in the local memory.
- **Remote:** When selecting **Remote**, the events are sent to the specified IP address and UDP port of the remote system log server.
- **Both:** When selecting **Both**, the events are recorded in the local memory or sent to the specified IP address and UDP port of the remote system log server.

After finishing setting, click the **Apply/Save** button to save and apply the settings.

✍ **Note:**

To log all the events, select the **Debugging** log level.

View System Log

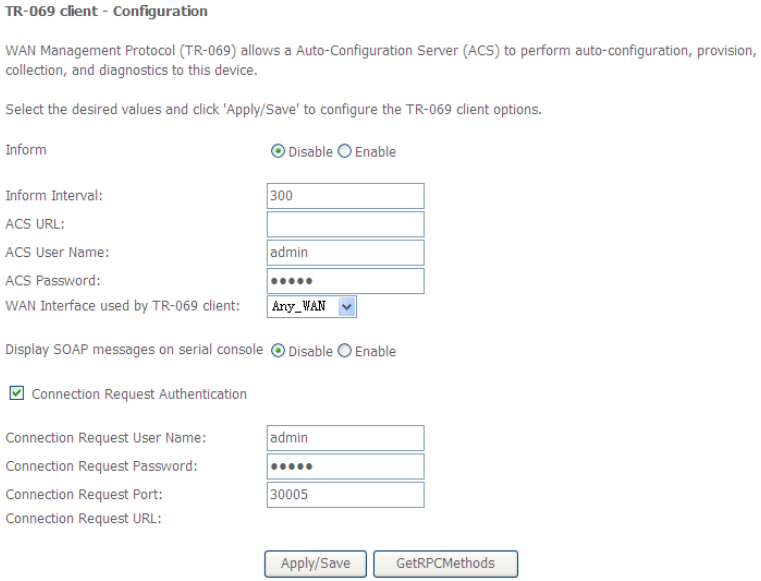
Click the **View System Log** button to display the following page.

In this page, you can view the system log.

Click the **Refresh** button to refresh the system log. Click the **Close** button to exit.

5.5.3 TR-069 Client

Choose **Management > TR-069Client** to display the following page.



WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

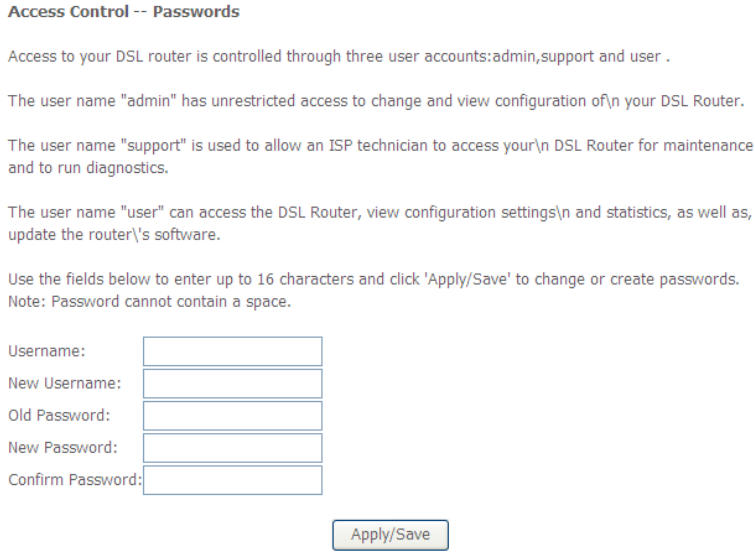
In this page, you may configure the parameters such as the ACS URL, ACS password and connection request user name.

After finishing setting, click the **Apply/Save** button to save and apply the settings.

5.5.4 Access Control

Passwords

Choose **Management > Access Control > Passwords**, and the following page appears.

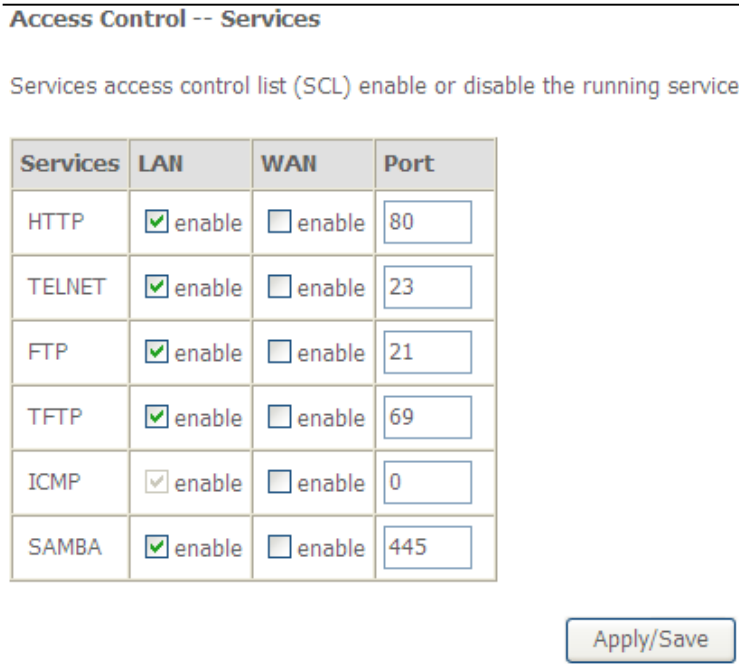

Access Control -- Passwords
Access to your DSL router is controlled through three user accounts:admin,support and user .
The user name "admin" has unrestricted access to change and view configuration of\n your DSL Router.
The user name "support" is used to allow an ISP technician to access your\n DSL Router for maintenance and to run diagnostics.
The user name "user" can access the DSL Router, view configuration settings\n and statistics, as well as, update the router\'s software.
Use the fields below to enter up to 16 characters and click 'Apply/Save' to change or create passwords.
Note: Password cannot contain a space.
Username:
New Username:
Old Password:
New Password:
Confirm Password:
Apply/Save

In the page, you can modify the username and password of different users.

After finishing setting, click the **Apply/Save** button to save and apply the settings.

Services Control

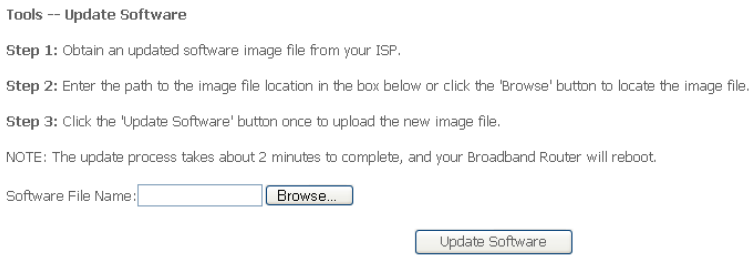
Choose **Management** > **Access Control** > **Services Control** and the following page appears.



In this page, you can enable or disable the different types of services.
After finishing setting, click the **Apply/Save** button to save and apply the settings.

5.5.5 Update Software

Choose **Management > Update Software**, and the following page appears.


Tools -- Update Software
Step 1: Obtain an updated software image file from your ISP.
Step 2: Enter the path to the image file location in the box below or click the 'Browse' button to locate the image file.
Step 3: Click the 'Update Software' button once to upload the new image file.
NOTE: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.
Software File Name:
Browse...
Update Software

To upload the software, click the **Browse…** button to choose the new software, and then click the **Update Software** button.

✍ **Note:**

When software update is in progress, do not shut down the router. After software update completes, the router automatically reboots. Make sure that the new software for updating is correct, and do not use other software to update the router.

5.5.6 Reboot

Choose **Management >Reboot** and the following page appears.

In this page, click the **Reboot** button, and then the router reboots.